Faculdade de Engenharia da Universidade do Porto

HP OpenView - Ferramentas Automáticas de Operação e Manutenção

Bruno José da Silva Brito

Dissertação do projecto realizado no âmbito do

Mestrado Integrado em Engenharia Electrotécnica e de Computadores

Major Automação

Orientador: Prof. Mário Jorge Rodrigues de Sousa

Porto 29 de Junho de 2009

MIEEC - MESTRADO INTEGRADO EM ENGENHARIA ELECTROTÉCNICA E DE COMPUTADORES **2008/2009**

A Dissertação intitulada

"HP OPENVIEW- FERRAMENTAS AUTOMÁTICAS DE OPERAÇÃO E MANUTENÇÃO"

foi aprovada em provas realizadas em 16/Julho/2009

o júri

Presidente Professor Doutor Paulo José Lopes Machado Portugal
Professor Auxiliar do Departamento de Engenharia Electrotécnica e de Computadores da Faculdade de Engenharia da Universidade do Porto

Professor Doutor Jaime Francisco Cruz Fonseca
Professor Associado do Departamento de Electrónica Industrial da Universidade do Minho

Professor Doutor Mário Jorge Rodrigues Sousa
Professor Auxiliar do Departamento de Engenharia Electrotécnica e de Computadores da Faculdade de Engenharia da Universidade do Porto

O autor declara que a presente dissertação (ou relatório de projecto) é da sua exclusiva autoria e foi escrita sem qualquer apoio externo não explicitamente autorizado. Os resultados, ideias, parágrafos, ou outros extractos tomados de ou inspirados em trabalhos de outros autores, e demais referências bibliográficas usadas, são correctamente citados.

Autor - **BRUNO JOSÉ DA SILVA BRITO**

Faculdade de Engenharia da Universidade do Porto

Resumo

Neste documento poder-se-á encontrar formas de monitorização de sistemas operativos e de aplicações adjacentes ao mesmo.

O trabalho realizado decorreu em ambiente industrial, tendo o mesmo sido implementado na empresa EDP, departamento de automação e telecontrolo.

No seu decurso será utilizada como ferramenta de apoio o software HP-OpenView, o qual proporciona uma implementação de monitorização compatível com os vários sistemas operativos presentes neste estudo, nomeadamente sistemas operativos Microsoft Windows e HP-UX 10.

Tendo-se como ponto de partida uma base de monitorização desactualizada, é efectuado um estudo de todas as normas de localização de anomalias, sua avaliação de eficácia e posterior adaptação para a realidade actual. Indo-se em vários casos um pouco mais a fundo sendo necessário o desenvolvimento de novas soluções de monitorização e de controlo, de forma a evitar a anomalia, ou caso em contrario atenuar o seu efeito nos restantes equipamentos da rede.

Abstract

This document gives an overview of the monitoring software HP-OpenView as it is used within EDP. It lists and documents basic operating systems performances processes, and the way they are used to anticipate the occurrence of failures.

In the study and implementation of the monitoring rules in the running machines, it focus on 2 operational platforms, Microsoft Windows and HP-UX, as well has the specially designed application GENESys, developed by EFACEC Portugal. On that bases the software implementations tries to improve the operating performances of the network as well as prevent breaks on the controlling platforms and the services presented by them.

Índice

Lista de figuras

Lista de tabelas

Abreviaturas e Símbolos

Lista de abreviaturas

IT	Tecnologias de informação
MTTR	*Mean Time To Repair*
OVO	*HP OpenView Operations*
OVOW	*HP OpenView Operations for Microsoft Windows*
RPC	*Remote Procedure Call*
SCADA	*Supervisory Control And Data Acquisition*
SSH	*Secure Shell*
VBScript	*Microsoft Visual Basic Scripting Edition*
WMI	*Windows Management Instrumentation*

Capítulo 1

Introdução

No âmbito da sua actividade, a EDP encontra-se espalhada por todo o país, interligando todos os clientes e satisfazendo as suas necessidades.

Esta relação prende-se com a existência de uma determinada comunicação energética entre o fornecedor e o comprador. Para tal, a EDP dispõe de um vasto conjunto de ramais eléctricos, subestações e postos de transformação que permitem não só adaptar as características de produção à realidade do consumo, mas também optimizar o valor de perdas energéticas neste percurso (fornecedor -> cliente).

Isto mesmo pode ser verificado a partir do esquema abaixo descrito na Figura 1.1.

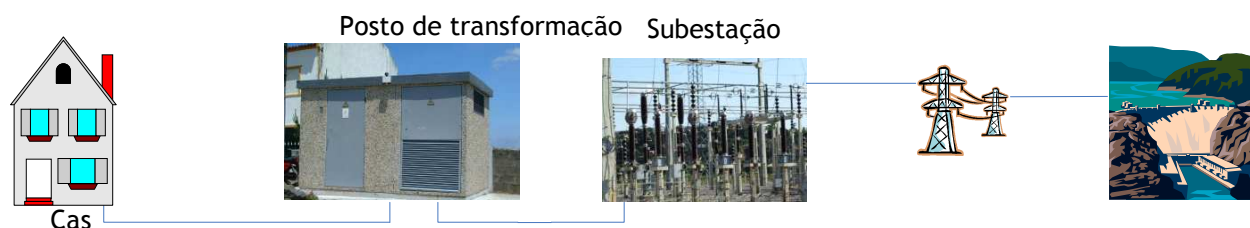



Figura 1.1 - Esquema da rede eléctrica

Nesta esquematização é de notar que o principal interessado na conexão acima descrita é o cliente/consumidor. Deste modo, o edifício onde o mesmo se encontra, está conectado por um cabo eléctrico, normalmente de 230V/410V (podendo ser possível também a existência de estabelecimentos alimentados a 15kV e 60kV). Este cabo está ligado a um quadro de colunas que agrega as várias baixadas dos clientes por zonas ou por ruas, dependendo da densidade de consumidores no local em análise.

Por sua vez, este quadro de colunas encontra-se conectado a uma subestação, por intermédio de um ou mais cabos eléctricos. Esta variação no número de cabos prende-se com o facto de um quadro poder ser permutado de uma subestação para outra, em caso de avaria.

Esta redundância deve-se à imposição legal de indicadores de qualidade, os quais são definidos por localização geográfica.

Esta rede faz a interligação entre várias subestações, as quais recebem energia através de cabos, sendo os mesmos de topologia maioritariamente aérea com tensões elevadas (acima dos 30kV). As subestações efectuam um abaixamento da tensão referida, distribuindo-a pelos condutores. Estes últimos ligam-se aos quadros de colunas por meio de tensões mais reduzidas (menores ou iguais a 15kV). No entanto, estas subestações recebem energia de várias proveniências: directamente de outras subestações, de produtores privados, de outras linhas particulares (REN - Rede Eléctrica Nacional), ou então de vários núcleos de produção que a EDP possui.

Para que a energia flua desde os produtores (barragens, centrais de combustão, eólicas, centrais solares, centrais de biomassa, entre outros) até as subestações, são alugadas linhas de alta tensão (400kV) à REN, sendo também usadas linhas de média tensão (15kV a 60kV) para se efectuar esse mesmo redireccionamento energético.

A gestão destes fluxos de energia é efectuada pelas áreas operacionais da empresa EDP, em colaboração contratual com a sua subsequente REN.

1.1. Suporte da rede eléctrica

Para ajudar no controlo de toda esta rede de cabos, disjuntores e outros aparelhos de medida e protecção, a EDP adquiriu da EFACEC uma solução, denominada de GENESys. Actualmente, esta encontra-se a controlar toda a rede energética da empresa EDP, possuindo para o efeito vários dispositivos lógicos.

A rede eléctrica nacional de baixa tensão possui instalados cerca de 62 mil PT’s (Postos de Transformação), dos quais apenas 400 destes se encontram monitorizados por autómatos programáveis, que comunicam com os servidores via rádio ou então através de um equipamento GSM (*Global System for Mobile communications*) (Figura 1.2). Estes autómatos contêm uma complexidade relativamente baixa, não possuem interface gráfica local para com o operador e podem ser actuados remota e localmente. Os mesmos podem também ser comandados pelo sistema da EFACEC sob uma forma global (usando uma interface de alto nível), ou sob uma forma automática, pois estes possuem diversas aplicações de segurança e protecção. Deste modo, nestas unidades é efectuada a redução da tensão de 15kV para os normais 240V das nossas casas.

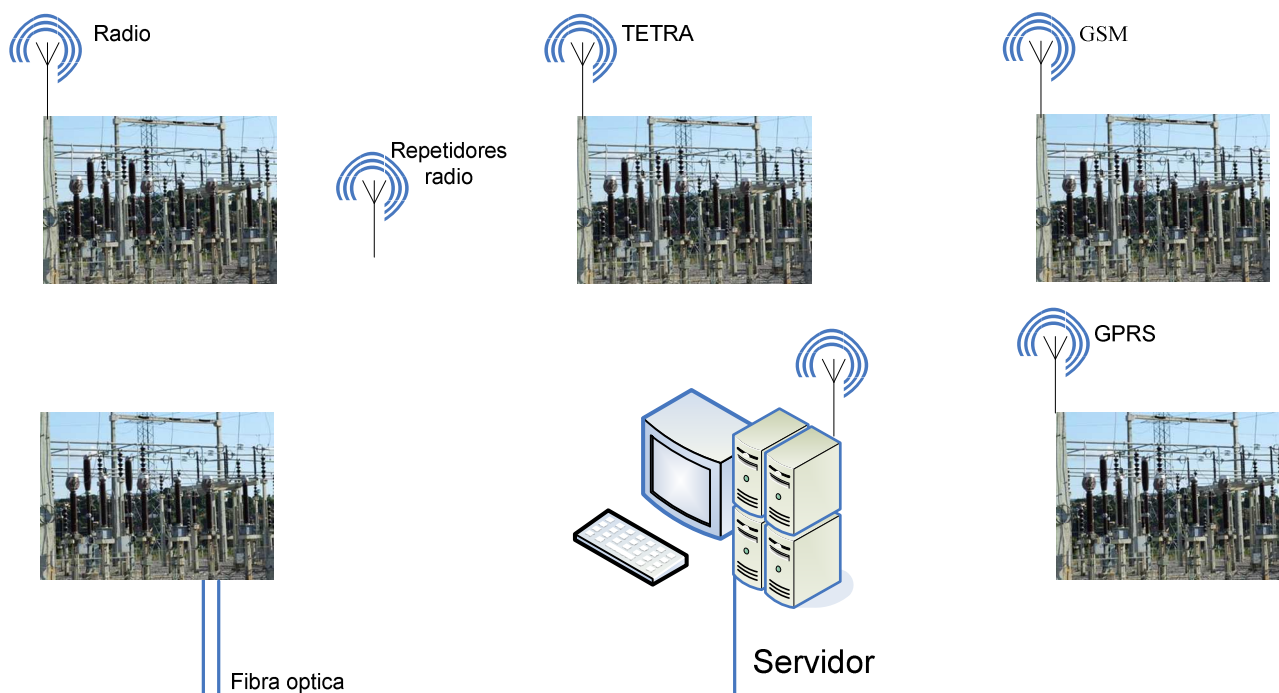



Figura 1.2 - Esquema de comunicação de controlo

Passando para o nível da rede eléctrica nacional de média tensão, temos à volta de 400 subestações distribuídas por todo o país. Estas instalações possuem uma maior complexidade, exigem um nível de controlo e comando bastante mais elevado, possuem interface gráfica para com o operador e podem ser comandadas local ou remotamente. Deste modo é utilizada uma aplicação da EFACEC, com base num computador industrial.

Esta interface gráfica é constituída da seguinte forma:

- Um sinóptico razoavelmente simples;
- Uma página de alarmes;
- Uma janela de *debugging*;
- Uma janela de monitorização de *couldstart's*;
- Uma janela de monitorização do protocolo de comunicação com o servidor;
- Uma janela de visualização das tramas para com os servidores;
- Uma janela de visualização de *debugging* dos processos de software.

Estas mesmas subestações comunicam com os servidores centrais a partir de protocolos fechados, sendo eles: IEC, CETT, PUR, EDP, TG809 e 4F.

Relativamente ao nível superior da gestão da rede eléctrica nacional, encontram-se instalados alguns equipamentos com determinadas funções específicas, tais como: a recepção, o tratamento e o armazenamento de dados da referida rede. Estes equipamentos serão descritos pormenorizadamente no decorrer deste documento.

1.2. Objectivos

No presente trabalho é explorada a plataforma de gestão, controlo e monitorização de redes HP-OpenView em sistemas operativos Microsoft Windows e Unix HP-UX, sendo desta forma estudados modelos de monitorização de variáveis de performance em programas e sistemas operativos. É também contemplada neste estudo a análise da monitorização da aplicação GENESys, desenvolvida pela EFACEC Portugal, na qual são desenvolvidas actualizações à monitorização existente e implementações de novas formas de avaliar as performances, com base na aplicação HP-OpenView.

Alguma informação é exposta sob forma tabelar, com o fim de mostrar não só as variáveis monitorizadas, como também o seu limite aceitável e crítico para o desempenho global de todo o sistema. Esta pode, em alguns casos, apresentar soluções pontuais, com o objectivo de minimizar ou evitar que a falha se propague e afecte sectores indesejados.

A proposta para a realização deste estudo consiste na identificação, actualização e desenvolvimento das monitorizações existentes no HP-OpenView para equipamentos dispersos. Esta mesma surge de uma necessidade de inovação e manutenção da já referida plataforma instalada na empresa EDP, uma vez que a aplicação nuclear GENESys da empresa teve uma actualização de versão. Isso mesmo levou a que, por sua vez, o controlo e a monitorização dos alertas gerados pela plataforma se encontrassem descontinuados. Este trabalho tem ainda como objectivo a implementação de novas ferramentas e funcionalidades.

Uma vez listadas as regras de monitorização existentes, estas são comparadas com os processos actualmente em execução nos equipamentos, possibilitando desta forma a identificação das alterações a serem efectuadas na implementação.

É ainda pedido, por parte da empresa EDP, a limpeza e filtragem das actuais mensagens internas geradas pelos agentes do HP-OpenView, pois para a empresa são consideradas irrelevantes e, até mesmo, prejudiciais para a determinação de anomalias na rede. A empresa propôs ainda a criação de várias ferramentas de ajuda ao suporte da rede, nomeadamente a implementação de acesso remoto aos seus equipamentos, a geração de cópias de segurança e a limpeza de ficheiros em disco, relacionando deste modo estes instrumentos com os nós onde as mesmas operam.

Fora ainda pedida a activação dos relatórios gráficos do HP-OpenView, a implementação de vários gráficos simples para avaliação das performances do equipamento em causa e a inicialização do acesso à consola Web da plataforma.

1.3. Estrutura

No presente documento a informação é tratada seguindo-se a estrutura apresentada: No capítulo 1 efectua-se, um enquadramento do funcionamento interno da empresa EDP, o âmbito que levou a elaboração deste trabalho nessa estrutura e os objectivos a atingir com a realização do presente trabalho. No capítulo 2 é efectuada uma descrição das várias plataformas existentes no mercado para a realização das tarefas propostas nos objectivos sendo dada uma especial atenção a plataforma HP-OpenView, pois a mesma é usada para a implementação do estudo realizado neste projecto.

O capítulo 3 documenta as ferramentas proporcionadas pela ferramenta, e as suas funcionalidades. O capítulo 4 bem no seguimento do trabalho realizado com as ferramentas do capítulo 3, bem como com algumas novas ferramentas descritas no capítulo 5, sendo que no capítulo 4 é efectuada a distinção entre o que já se encontrava implementado e as alterações efectuadas para uma melhor monitorização dos equipamentos.

No capítulo 5 são descritas várias ferramentas implementadas, algumas das quais para monitorização de processos e aplicações, sendo as restantes implementadas com o objectivo de melhorar a performance dos equipamentos e optimização de tarefas de manutenção.

O capítulo 6 descreve de uma forma sucinta algumas implementações de scripts em *batch*, sendo este capítulo dividido em duas partes, tratando-se na primeira de scripts em ambientes Microsoft Windows e na segunda de scripts em Unix, tendo sido os dois ambientes de monitorização utilizados neste trabalho.

No capítulo 7 é efectuada uma conclusão final, apresentando as vantagens da implementação efectuada e propostos vários trabalhos para desenvolvimento futuro.

Capítulo 2

Ferramentas de Gestão Centralizada

Num ambiente em que, cada vez mais, os programas são multi-plataforma, correndo em máquinas com variadas especificações e objectivos, em sistemas operativos diferentes, com inúmeros processos deslocalizados e repartidos, surge a necessidade de se monitorizar a evolução global do sistema para, em caso de necessidade, se identificar rápida e facilmente os sectores em anomalia.

Com o fim de se obter maior capacidade de processamento, são usados e distribuídos variados processos por diversos processadores de uma mesma máquina, ou então, por máquinas diferentes, levando desta forma ao aparecimento de novos equipamentos com funções específicas e com uma maior robustez de implementação, devido ao facto de se poderem deslocalizar processos de uma mesma aplicação.

Actualmente, este tipo de solução tem vindo a ser utilizada, visto que os programas informáticos para realização de uma determinada tarefa adquiriram um tamanho e complexidade de tal forma superior que o poder computacional de um só equipamento não garante uma resposta eficaz.

Nesta concepção encontra-se então a empresa EDP, usando uma solução dedicada ao seu modelo de negócios para controlo e monitorização de vários dos seus equipamentos de campo. É de notar que estes equipamentos se encontram espalhados por todo o país, em zonas de difícil acesso e conectividade (a rede móveis inclusivé) e onde as ligações a redes físicas são inexistentes.

Como tal, surge a solução SCATEX implementada pela EFACEC, desenhada especialmente para o mundo de controlo de redes eléctricas, onde se encontra inserida a empresa EDP. Este programa assenta numa interface tabelar nacional entre várias máquinas descentralizadas, com o fim de efectuar a aquisição de dados, entre quais se destacam: valores de tensões, correntes e potências activas e reactivas.

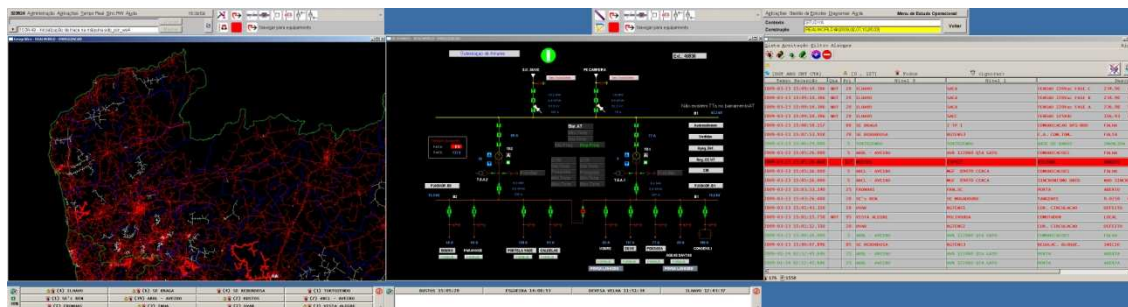



Figura 2.1 - Interface GENESys para com o utilizador

Com a evolução tecnológica desencadeia-se uma necessidade de actualização desta plataforma, sendo então pedido novamente à EFACEC que efectue esta remodelação, a qual dá origem ao sistema de controlo GENESys (Figura 2.1).

Esta nova plataforma implementa uma solução ainda mais complexa que a existente até então, sendo não só necessário a actualização do software, como também do hardware nas diferentes máquinas, de forma a suportar as novas características, permitindo assim manter uma solução fiável com uma resposta temporal aceitável para o controlo do processo.

2.1. Necessidade de uma ferramenta de Gestão Centralizada

Aquando da implementação desta solução de controlo, a maioria dos servidores tiveram que ser monitorizados, tarefa que se torna relativamente incómoda devido à necessidade de ter que estar presente um utilizador a observar o correcto processamento de cada máquina. Esta situação aconteceria num cenário onde as máquinas estivessem acessíveis para inspecção directa. No entanto, geralmente este caso não se verifica, pois grande parte destes equipamentos encontram-se colocados em armários '*Rack*', os quais não dispõem de monitores para monitorização.

Para se ultrapassar este problema, a EDP implementou três tipos de soluções: uma baseada em *RemoteDesktop* para máquinas com sistema operativo Microsoft Windows XP; uma outra baseada em NetMeeting e VNC para computadores cujo sistema operativo seja Microsoft Windows NT 4.0; e ainda uma outra utilizada para sistemas operativos HP-UX baseada na ligação por SSH ou Telnet.

Consequentemente, com esta actualização, os equipamentos passaram a poderem ser controlados, acedidos e, até mesmo, executados remotamente a partir de máquinas diferentes, proporcionando assim uma maior flexibilidade de manutenção e rapidez na sua intervenção.

Como é evidente, um administrador de redes não pode efectuar a monitorização de todas as aplicações, processos e variáveis contidas em todos os equipamentos, em tempo real sendo, por isso, necessária uma solução que monitorize o hardware, o sistema operativo e o software de todos esses equipamentos, e que informe atempadamente o administrador de possíveis anomalias.

2.2. Ferramentas de controlo centralizado

Para a implementação de um sistema de controlo centralizado, é necessário conhecer a rede à qual o mesmo será aplicado, possibilitando assim a escolha da melhor decisão, aquando da compra da referida solução.

Após uma análise do mercado mundial referente a este género de solução, encontram-se alguns tipos de implementações possíveis, que serão descritos seguidamente no presente capítulo. Aí, serão também enumeradas as vantagens e desvantagens da implementação de cada um na rede.

2.2.1. HP OpenView

O HP OpenView trata-se de uma implementação já madura da HP com um histórico de mais de 15 anos. Este resulta da interligação de conhecimentos obtidos através de várias empresas pela HP, proporcionando-lhe não só manter-se na liderança tecnológica, mas também afastar a concorrência neste sector.

Para além disto, o HP-OpenView dispõe de um conjunto de módulos de outras empresas que, em associação com a HP, lhe disponibilizam o conhecimento das suas aplicações, de modo a permitir a possibilidade de utilização de funções importantes na monitorização, bem como controlar e optimizar as performances dos equipamentos monitorizados. Destes associados salientam-se os seguintes:

- Adobe® , Acrobat®, e-Adobe Systems Incorpodated
- Java™
- Microsoft e Genuine Microsoft Products
- MS-DOS®, Windows®, Windows NT® e MS Windows da Microsoft Corporation
- Netscape, Netscape Commerce Server, Netscape Navigator e Netscape Proxy Server
- Oracle®
- Oracle Reports™, Oracle7™ e Oracle7 Server™
- OSF, OSF1 e OSF/Motif da Open Software Foundation
- Pentium® da Intel Corporation

- UNIX da The Open Group

É de notar a existência de outras empresas que divulgam abertamente todas as informações úteis para a monitorização de seus produtos e, por esse mesmo motivo, estas não são oficialmente citadas. No entanto, é reconhecida a interligação destas para com a plataforma do HP-OpenView, fornecendo-lhe uma forma de monitorização fiável, robusta e credível.

Deste modo, o software da HP encontra-se dividido em módulos que poderão ser adquiridos separadamente, oferecendo as mais variadas configurações aos seus demais clientes, permitindo assim uma escolha mais próxima das suas necessidades.

Estes módulos, que podem funcionar não só individualmente, mas também de forma colectiva, permitem efectuar a monitorização das máquinas, realizar tarefas periódicas e observar o tráfego da rede de informação, detectando pontos de estrangulamento ao longo desta.

Módulos do HP OpenView disponíveis no mercado:

- HP OpenView Network Node Manager (OV NNM);
- HP OpenView Operations (OVO) — monitoriza sistemas e aplicações utilizando agentes para Windows (OVOW) (antigo VantagePoint Operations para Windows) e Unix 8.1 (OVOU) (antigo VantagePoint Operations para Unix, algumas vezes referenciado como ITO – Information Tecnology Operations);
- HP OpenView ServiceCenter (antigo Peregrine ServiceCenter) – agora HP Software Service Manager;
- HP OpenView AssetCenter (antigo Peregrine AssetCenter)
- HP OpenView Service Desk (OVSD) - descontinuado
- HP OpenView Internet Services (OVIS) - descontinuado
- HP OpenView Service Navigator (integrado em HP Operations Manager para Unix desde 1996)
- HP OpenView Transaction Analyzer (OVTA) - descontinuado
- HP OpenView SOA Manager
- HP OpenView Select Identity (OVSI) - descontinuado
- HP OpenView Select Access (OVSA) - descontinuado
- HP OpenView Select Audit - descontinuado
- HP OpenView Select Federation - descontinuado
- HP Software Universal CMDB (uCMDB)

Devido à complexidade e variedade de configurações existentes, esta ferramenta torna-se complexa de implementar e de monitorizar, levando à necessidade imediata de uma avaliação diária do sistema por um especialista.

2.2.2. IBM Tivoli

Trata-se também de um software de monitorização utilizando agentes, que permite uma melhor actuação sobre os equipamentos monitorizados, de forma a reduzir o tempo médio de reparação, detectando-o aquando da sua existência ou prevenindo o seu aparecimento com antecedência. O mesmo contempla ainda a criação de gráficos estatísticos e emite avisos em caso de anomalias.

Suporta as mais variadas tecnologias, sistemas operativos e softwares, como se pode observar na sua listagem de suporte:

AIX	HP-UX
Solaris	IBMi5/OS™
Windows	DB2
Linux (Red Hat, SUSE) em processadores Intel	Microsoft SQL Server
® IBMSystemz™	Oracle
IBMSystemp™	Sybase

Quanto à sua estrutura interna, este encontra-se separado em vários módulos (tal como acontece na maioria dos gestores de tecnologias de informação), possibilitando assim a aquisição de apenas um ou de vários módulos, conforme as necessidades do utilizador, podendo ser facilmente adaptada uma solução específica a cada cliente.

Abaixo encontram-se descritos os módulos que se regem pelo IBM Tivoli.

- Tivoli Monitoring Software e Tivoli Performance Analyzer;
- TivoliMonitoring Agents:
- IBMTivoliMonitoring para Active DirectoryOption
- IBMTivoliMonitoring para Applications
- IBMTivoliMonitoring para ClusterManagers
- IBMTivoliMonitoring para DB2, Oracle, Microsoft SQL Server e Sybase
- IBMTivoliMonitoring para Messaging and Collaboration
- IBMTivoliMonitoring para Virtual Servers

Este sistema permite ainda a fácil implementação e gestão de regras ao ser utilizado um ambiente muito intuitivo, o que faz com que um operador com poucos conhecimentos sobre o funcionamento da aplicação possa monitorizar a infra-estrutura de IT onde este se encontra parametrizado.

2.2.3. ManageEngine- OpManager

Esta solução de gestão descentralizada oferece o menor custo tendo, por esse mesmo motivo, preços atractivos para vários sectores empresariais. Estes custos dependem dos módulos da aplicação necessários para o controlo e monitorização bem como do número de máquinas a monitorizar.

Como tal, a solução implementada no *OpManager* disponibiliza vários módulos de monitorização, controlo e apresentação para cada uma das áreas mais críticas das redes de IT. Esta aplicação trata-se de um sistema único, que fornece os mais diversos componentes de controlo aquando da sua instalação, proporcionando assim uma implementação mais poderosa e eficaz quando se pretende gerir uma plataforma com poucos recursos. A mesma teve um amadurecimento progressivo ao longo dos anos, encontrando-se actualmente na oitava versão de lançamento, a qual é bastante estável e possui um grau de fiabilidade e consistência elevado.

O *OpManager* apresenta suporte para os seguintes sistemas operativos:

- Microsoft -> Windows 2003 Server, Windows 2000 Server, Windows XP, Windows 98, Windows Vista.
- Linux –> Distribuições de Linux com suporte glibc versão 2.3 (ou superior) ou com suporte X Libraries.
- Explicitamente não suporta – FreeBSD, Solaris.

Ao observar-se esta lista, é de notar a falta não só de componentes para sistemas operativos normalmente usados em servidores, mas também de monitorização de bases de dados e da estrutura de redes por SNMP.

2.2.4. iREASONING Networks - SysUpTime

Trata-se de uma implementação de custo muito reduzido para pequenas empresas, que suporta sistemas operativos como Microsoft Windows, Mac OS X, Linux e outras plataformas UNIX. A mesma decompõe-se em vários módulos, podendo os seus utilizadores adaptarem com mais facilidade uma solução para melhorar a gestão da sua rede de IT.

Módulos disponíveis:

- MIB Browser
- SNMP API
- SNMP Agent Builder
- SNMP Agent Simulator
- SysUpTime Network Monitor
- SysUpTime MSP Edition

- TL1 API

2.2.5. Blue Elephant Systems - MIDAS

Esta aplicação apenas ajuda na criação e gestão de políticas de monitorização. No entanto, como não se trata de um sistema *stand alone*, é necessária a instalação prévia do HP-OpenView para que a mesma funcione.

Esta solução desenvolve-se numa camada superior ao HP-OpenView, onde se pode implementar um maior número de funcionalidades, um ambiente gráfico mais intuitivo e diversos relatórios já pré-concebidos. Contudo, para a criação desta implementação na plataforma nativa do HP-OpenView, é necessário despender um elevado período de tempo no seu desenvolvimento. Deste modo, a MIDAS alarga o leque de soluções do HP-OpenView, como se de mais um dos seus módulos se tratasse.

2.2.6. BMC Performance Management

A solução proposta pela BMC para gestão de tecnologias de informação descentralizadas dispõe de meios proactivos de detecção, diagnóstico, isolamento e correcção de problemas na infra-estrutura proporcionando, desta forma, uma elevada estabilidade nos serviços. É de notar que na possibilidade de ocorrerem várias anomalias em simultâneo, os serviços principais que garantem o núcleo do negócio continuam em funcionamento não permitindo, deste modo, que o utilizador consiga ver a anomalia em causa, utilizando o pressuposto para garantir uma arquitectura redundante de equipamentos.

O seu mecanismo de detecção permite identificar antecipadamente falhas e eventuais causas das mesmas, oferecendo assim uma manutenção mais eficaz e preventiva.

Esta plataforma assenta num algoritmo de aprendizagem, o qual monitoriza o trabalho diário, adaptando-se de forma automática às necessidades da rede onde se encontra implementado, conseguindo assim uma redução do MTTR. A mesma integra os mais variados sistemas operativos existentes no mercado, facilitando a monitorização das mais diversas máquinas, sem serem necessárias grandes pré-adaptações e conhecimentos sobre o funcionamento das redes existentes na empresa.

Esta solução é disponibilizada em vários módulos adquiridos separadamente, de forma a estar em conformidade com as necessidades do cliente. A utilização de empresas parceiras permite uma maior integração com os recursos de IT do cliente, um elevado poder de avaliação das performances monitorizadas e uma melhor segurança na determinação de irregularidades que poderão causar a instabilidade do serviço.

2.3. Escolha da plataforma HP-OpenView para monitorização

A empresa EDP optou pela escolha do HP-OpenView como plataforma de gestão, em 2001, com o objectivo de, não só rentabilizar os equipamentos instalados, mas também de detectar e quantificar anomalias (como o caso de quebras de serviço e indisponibilidades) na sua rede interna, de uma forma mais rápida e eficaz. Contudo, esta aquisição não se ficou apenas pela monitorização da eficiência da rede. A mesma pode intervir, evitando em muitos casos que a anomalia aconteça. Isto deve-se ao facto de existir um mecanismo interno, que permite a execução de pequenas aplicações especialmente concebidas para o restauro e reabilitação do equipamento.

Esta plataforma fora inicialmente instalada em dois pólos (norte e sul), uma vez que a gestão da rede da EDP se encontrava isolada entre esses mesmos pólos. Com a posterior fusão dessas duas entidades, as características da rede alteraram-se, sendo efectuada a conexão das duas redes, centralizando os serviços num único pólo, estando este localizado em Palhavã (Lisboa).

Com esta nova topologia da rede, um dos primeiros equipamentos a sofrer alterações foi o HP-OpenView. Deste modo, ao ser desactivado o servidor norte, todos os agentes por este monitorizados foram comutados para o servidor sul, levando à implementação neste último de todas as políticas e ferramentas existentes no servidor a norte.

Futuramente, os objectivos desta grande empresa serão a possibilidade de comutação de servidores entre os dois pólos, podendo qualquer um dos dois assumir o controlo da rede na íntegra, proporcionando desta forma uma recuperação garantida em caso de catástrofe.

Capítulo 3

HP-OpenView

O HP OpenView é um software da empresa Hewlett-Packard, tendo a sua primeira versão comercial sido apresentada em 1994.

Suportava inicialmente HP-UX, ambientes MSDOS e Windows V3.1, efectuava uma monitorização usando WINSOCK, e SNMP. Inicialmente estava projectado para monitorização de redes em TCP/IP e IPX, este podia monitorizar entre 6 a 10 segmentos de rede, de acordo com o equipamento base onde se encontrava instalado.

Com as novas actualizações o mesmo veio a usufruir das mais variadas aplicações isto em grande parte dependendo de acordos com empresas de hardware e software por parte da HP, bem como da compra de várias empresas, estas também no ramo do software de monitorização, anexando módulos das mesmas á sua versão base do OpenView.

A solução actualmente comercializada conta com a parceria de empresas de renome internacional, no desenvolvimento de aplicações e de hardware de alto desempenho e fiabilidade, como é o caso da Cisco Systems, Oracle, Microsoft, Sun, IBM, entre outras. Esta aplicação possibilita a monitorização de um número virtual de equipamentos, estando este número apenas dependente da máquina de operação e das suas capacidades da rede. A aplicação encontra-se pois fraccionada em vários módulos, demarcando-se os módulos operacionais que permitem a visualização por parte dos operadores dos módulos de monitorização instalados nos equipamentos, estes denominados de agentes, possibilitam uma poupança económica ao se poder modelizar a aplicação de controlo apenas aos módulos existentes na empresa.

È ainda interessante o facto da solução HP-OpenView ter evoluído não só a nível de monitorização, mas também de controlo, possibilitando assim a realização á distancia de várias tarefas, como é o caso da instalação e actualização de aplicações, configuração de novos utilizadores de novos equipamentos e a realização de um levantamento contínuo dos equipamentos ligados na rede.

3.1. Princípio de funcionamento

No desenvolvimento da aplicação de monitorização centralizada, os engenheiros da HP tiveram em conta a mobilidade e versatilidade da aplicação, tendo então implementado uma solução que permite a aquisição modelar de diversos componentes (Figura 3.1). Sendo o HP-OpenView Operations essencial para a interligação destes módulos e estando este dependente de outros módulos como é o caso dos agentes e das consolas de tratamento e pré-processamento de informação, como por exemplo a consola de NNM (*Network Node Manager*) e de estruturas de base de dados.

O núcleo central do HP OpenView é conhecido como *Operations*, sendo que este módulo apenas efectua a agregação, modelização e organização da informação recolhida para disponibilizar ao operador e para interligação com outros módulos, como é o caso do arquivo em base de dados Microsoft SQL Server. Para a aquisição da informação o HP OpenView vem munido com vários módulos denominados Agentes. Sendo que os agentes poderão ser adquiridos para a monitorização das mais diversas aplicações, não descartando o agente básico que efectua a monitorização do sistema operativo.

A monitorização do sistema operativo é pois feita com recursos às variáveis de sistema, de onde se destaca a aplicação da Microsoft WMI, já pré-embebidos no sistema operativo Microsoft Windows. Esta aplicação é pois apresentada ao utilizador comum com o comando 'WMIC, e em conjunto com os ficheiros de registo de anomalias e de eventos proporcionam uma monitorização avançada e de elevada fiabilidade. Os agentes de sistemas operativos não estão só preparados para a monitorização, estes também executam o comando de tarefas de controlo previamente agendadas, servindo-se da aplicação '*Scheduled Tasks*' presente no painel de controlo do Windows e permitindo a execução de comandos ou scripts aquando de um evento ou periodicamente.

Este agente de monitorização de sistemas operativos Microsoft Windows não se trata do único agente base fornecido pela HP, existindo ainda o agente de base para ambientes Unix, Linux e Solaris Operating System. Os mesmos baseiam-se e utilizam ferramentas já existentes no próprio sistema para registarem e comandarem os processos em execução, ferramentas que têm sido desenvolvidas pelas mais diversas empresas e embebidas nos sistemas de acordo com contractos de parceria entre estas empresas de desenvolvimento de software e as empresas que desenvolvem software de monitorização e controlo.

Para além dos agentes básico essenciais na monitorização e controlo de sistema operativo de suporte, o HP OpenView disponibiliza também agentes de monitorização específicos para as mais diversas aplicações, como é o caso do agente para bases de dados Oracle, para bases de dados MySQL e Microsoft SQL Server, agentes de monitorização de redes como é o caso dos

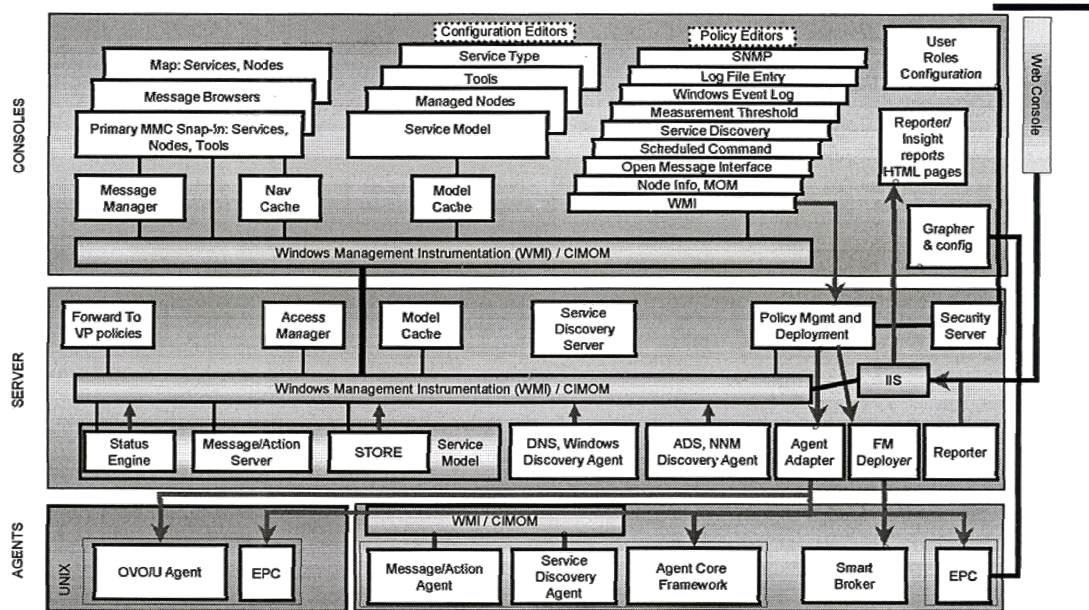



Figura 3.1 - Esquemático de funcionamento do HP-OpenView.

agentes SNMP em conjunto com a aplicação de processamento NNM, agentes de monitorização de hardware como o caso de UPS, routers, switch e de impressoras, bem como uma vasta gama de outros equipamentos passíveis de serem monitorizados e controlados por meios indirectos por um ou mais destas soluções.

3.2. Tipos de monitorização

O HP-OpenView implementa uma monitorização orientada por regras pré definidas pelo utilizador. Regras que de uma forma muito particular surgem da necessidade de se observar a progressão das enumeras possibilidades de pontos de ruptura, falha ou anomalia, não apenas no sistema operativo que suporta a nossa aplicação, mas também da própria aplicação, suas redes de suporte e infra-estruturas adjacentes.

Para uma melhoria de utilização e implementação, a HP na criação do OpenView distinguiu diferentes tipos de regras, agrupandas em políticas de monitorização. Políticas que fazendo uso do conjunto de regras avaliam de uma forma lógica várias tarefas desempenhadas, sendo estas tarefas de interesse e relevância para o funcionamento das aplicações de suporte ao negocio da empresa EDP. Nota-se uma breve semelhança do conjunto de regras que formam as políticas mais directas com a formulação das regras numa dinâmica Fuzzy.

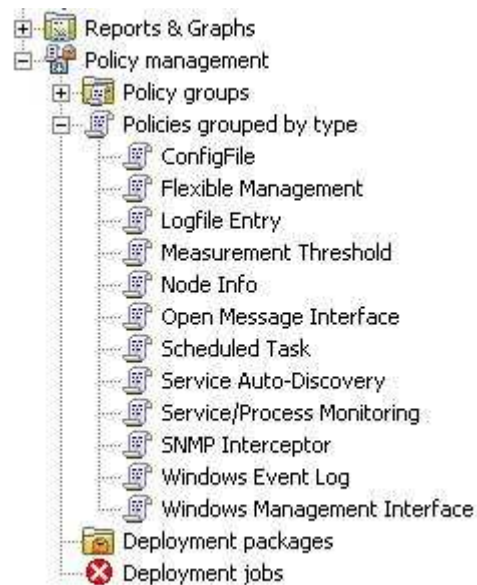



Figura 3.2 - Formas de monitorização

Com o agrupar de regras a políticas (Figura 3.2), as políticas passam então a poder enviar avisos ao operador quando as regras existentes em cada política suplantarem a formulação programada. Esta quebra detectada no normal funcionamento poderá estar definida em vários níveis de avisos uma vez que parte destas políticas não representam uma decisão binária mas sim progressiva gerando mensagens ao operador de acordo com os vários níveis de gravidade predefinidos na política.

O HP-OpenView não se completa apenas com a aplicação de regras numéricas de limites, existindo diferentes categorias de regras para diferentes fins e para a monitorização de diferentes tipos de sistemas.

Os diferentes tipos de políticas e possíveis regras encontram-se descritas nos pontos seguintes.

3.2.1. Config File

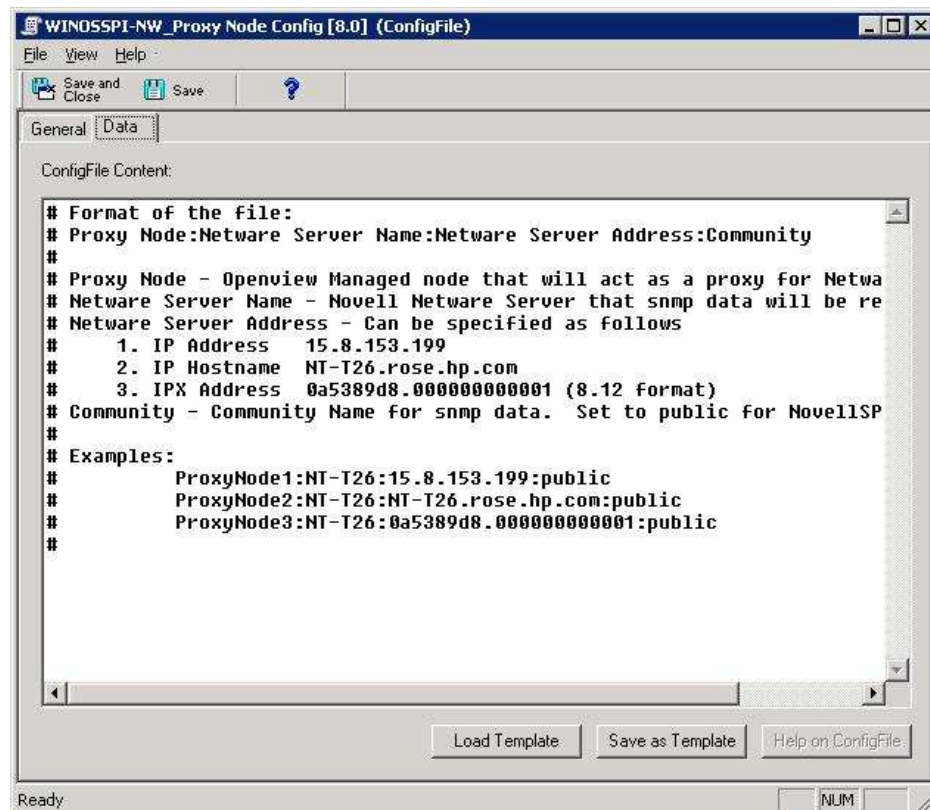



Figura 3.3 - Configurações de política *Config File*

Esta política está relacionada apenas com os agentes UNIX permitindo em conjunto com a aplicação 'OSSPI' do agente realizar vários tipos de configurações automaticamente aquando da ligação de um equipamento UNIX na rede monitorizada pelo OpenView.

Estas alterações poderão passar por configurações de rede, configurações de aplicações para funcionamento na rede entre outras soluções de configuração.

No seu funcionamento esta política contém os ficheiros de configuração, e de aplicações (Figura 3.3) já programados sendo apenas os mesmos ligeiramente adaptados ao equipamento detectado e colocados nos repositórios de onde as aplicações vão ler esta informação.

3.2.2. Flexible Management

A política Flexible Management permite ajustar previamente a gestão dos equipamentos, ao se poder definir que utilizador tem permissões para executar determinada aplicação, aceder a directorias e alteração de ficheiros. Permite ainda a configuração de data e hora do equipamento e alteração dos atributos das mensagens geradas pelos agentes (Figura 3.4).

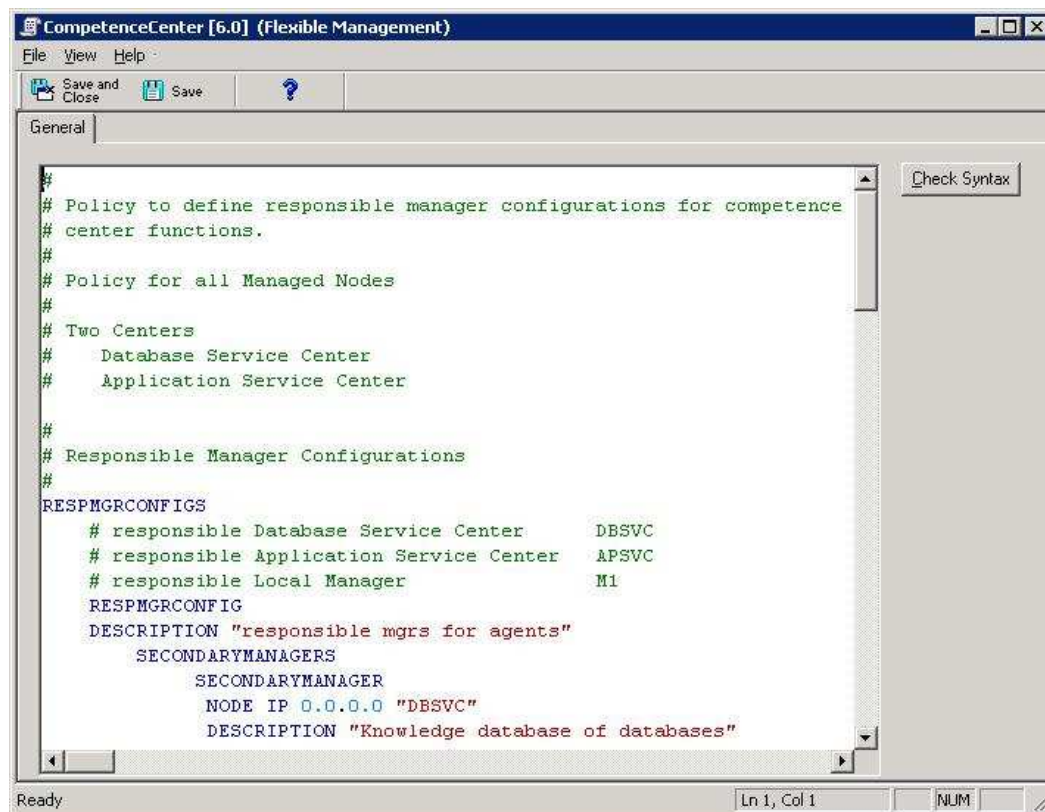



Figura 3.4 - Configurações de política *Flexible Management*

Basicamente esta política funciona como um agente flexível de onde o operador do equipamento poderá aceder e não apenas a aplicação HP-OpenView.

3.2.3. Logfile Entry

A maioria das aplicações em comercialização produz ficheiros de registo de ocorrências, onde guardam as anomalias e anotações de *debugging* para numa fase de análise de erros se determinar as funções internas que geraram e levaram a paralisação, ou realização de saídas inesperadas.

A monitorização destes ficheiros de registo de anomalias produzidos pelo sistema operativo ou por uma aplicação é de extrema importância, pois apesar de todos os indicadores poderem-se encontrar dentro dos limites considerados como normais de funcionamento na realidade a aplicação poderá estar em anomalia.

Nestes ficheiros normalmente consta informação essencial para a gestão da plataforma de tecnologias de informação, destacando-se a necessidade de aquisição da informação contida nos mesmos e reflectindo-se a existência desta política. A implementação da política encontra-se preparada para ler ficheiros em vários modos, e em vários formatos, disponibilizando ainda a hipótese de se executar aplicações de conversão de ficheiros para formatos conhecidos pelo agente, efectuando a posterior leitura destes ficheiros gerados.

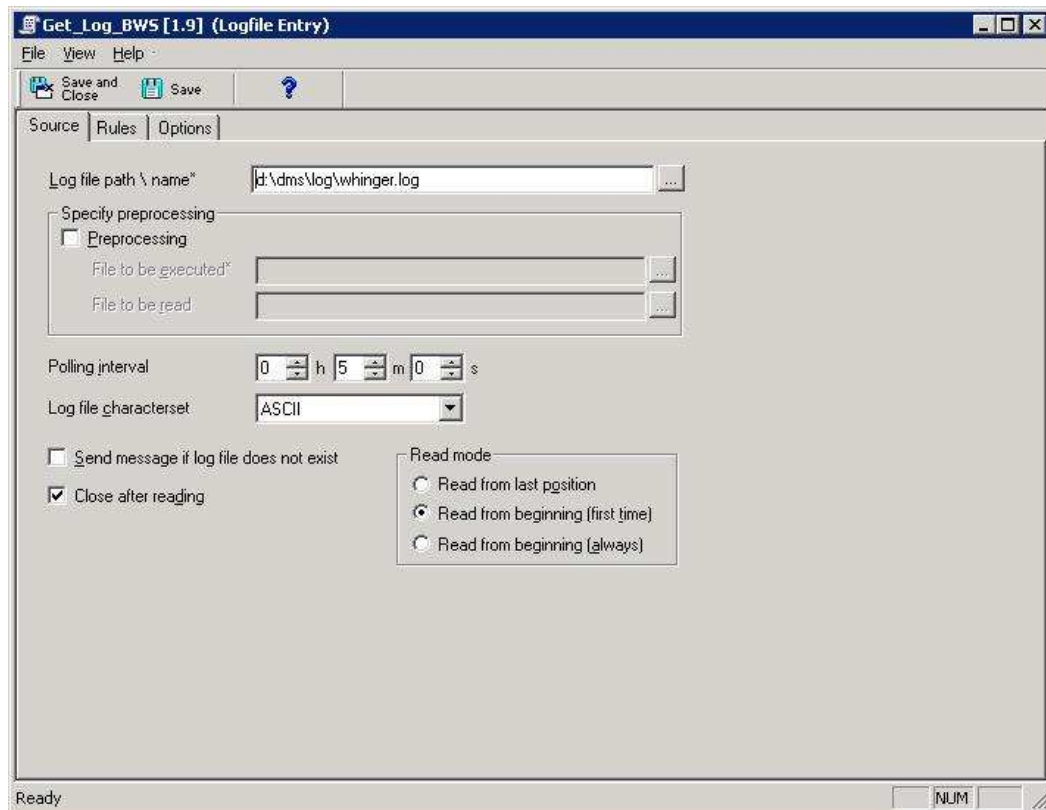



Figura 3.5 - Configurações de política *Logfile Entry*

Na leitura dos mesmos ficheiros ainda existe a possibilidade de se ler o ficheiro do inicio a cada execução da politica (Figura 3.5), apenas do ponto de ultima inspecção ou mesmo apenas a ultima inserção no ficheiro, isto possibilitando uma vasta gama de implementações. Sendo a informação recolhida analisada e enviada ao servidor por mensagens, onde este poderá observar o normal funcionamento das aplicações e detectar possíveis pontos de anomalia, reportando o mesmo acontecimento ao operador que após uma análise do problema irá tomas um conjunto de medidas como informar a empresa que desenvolveu o software ou mesmo procedendo a sua correcção para evitar futuras repetições.

3.2.4. Measurement Threshold

A implementação deste tipo de políticas tem como base regras de variáveis quantificáveis. A mesma poderá detectar quedas para valores inferiores ou incrementos para valores superiores, isto em conjunto com pequenos scripts, programados para contar elementos, como por exemplo o número de processos, esta poderá ser usada para

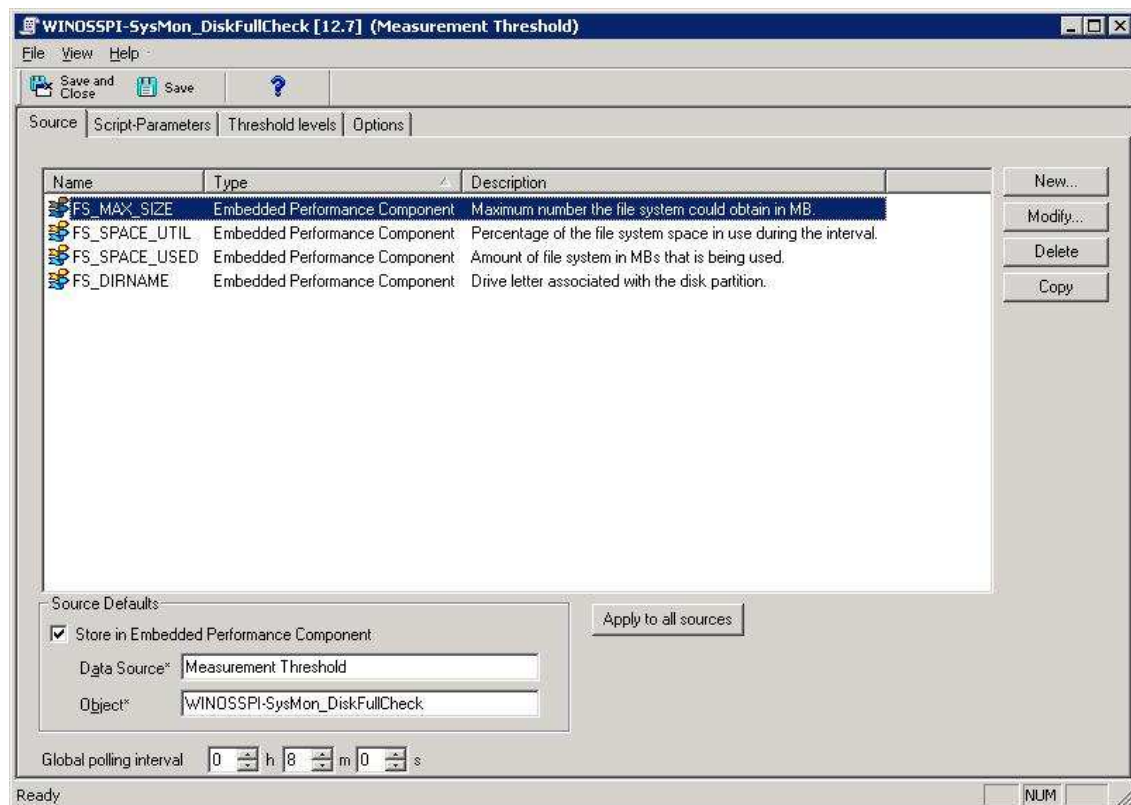



Figura 3.6 - Configurações de política *Measurement Threshold*

determinar e monitorizar uma grande parte efectiva dos sistemas que se encontram em execução. De notar que variáveis binárias são comparadas normalmente, e usadas como uma ocorrência excepcional destas regras (Figura 3.6).

A interligação em simultâneo de várias regras permite estar a monitorizar vários processos podendo as mesmas em caso de anomalia enviar uma mensagem com a indicação de que a aplicação monitorizada poderá estar em perigo ou mesmo em anomalia, isto apenas com uma política indexada a várias regras.

As regras desta política encontram-se directamente ligadas aos agentes podendo adquirir valores de pequenos scripts, variáveis do sistema operativo como o caso da ferramenta WMI em Microsoft Windows, e muitas mais origens dependendo do agente em que a política se encontrar.

3.2.5. Node Info

Trata-se não de uma política de monitorização mas sim da configuração do agente instalado.

Os agentes quando são instalados no equipamento criam um ficheiro de configurações *'nodeinfo'*, estas configurações afectam a execução do agente ao nível das suas variáveis internas (Figura 3.7) podendo-se definir valores para as mesmas, bem como a alteração de parâmetros.

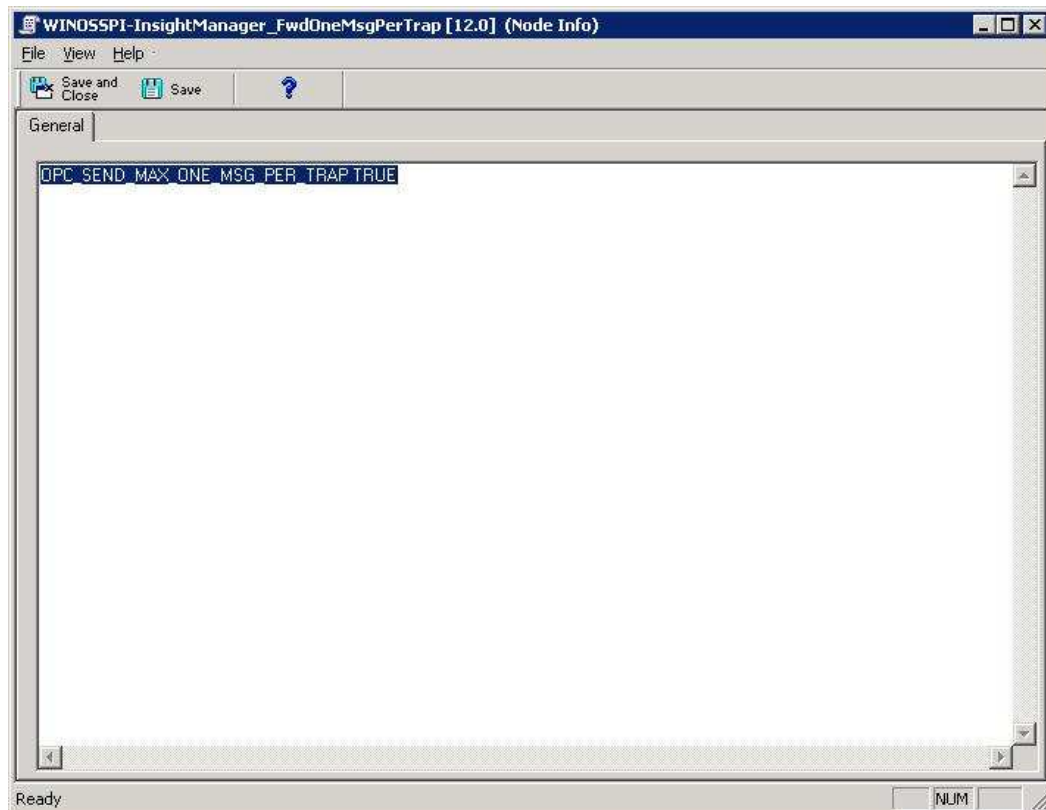



Figura 3.7 - Configurações de política *Node Info*

Este ficheiro é alterado aquando da distribuição desta politica com os novos parâmetros, sendo os parâmetros restituído á sua forma original aquando da inactivação da política.

Esta política necessita de um conhecimento prévio do funcionamento dos agentes bem como das suas configurações antes do mesmo ficheiro ser alterado.

3.2.6. Open Message Interface

Esta política tem como regras de entrada mensagens geradas por outras políticas, sendo de extrema utilidade aquando de uma avalanche de mensagens de aviso ao operador. A criação de uma política desta natureza permite pois programar e apenas enviar uma mensagem ao utilizador suprimindo todas as outras, informando do que realmente se encontra em anomalia e escondendo todos os processos e aplicações que geram erros partindo desta mesma origem.

È consequentemente usada ainda para reflectir o estado actual dos serviços ao aglomerar mensagem de diferentes aplicações, como exemplo da base de dados e da aplicação que faz uso da mesma. Ambas emitiram mensagens de anomalias, mas a causa poderá ser a base de dados com erro, alastrando-se a aplicação que a usa (Figura 3.8).

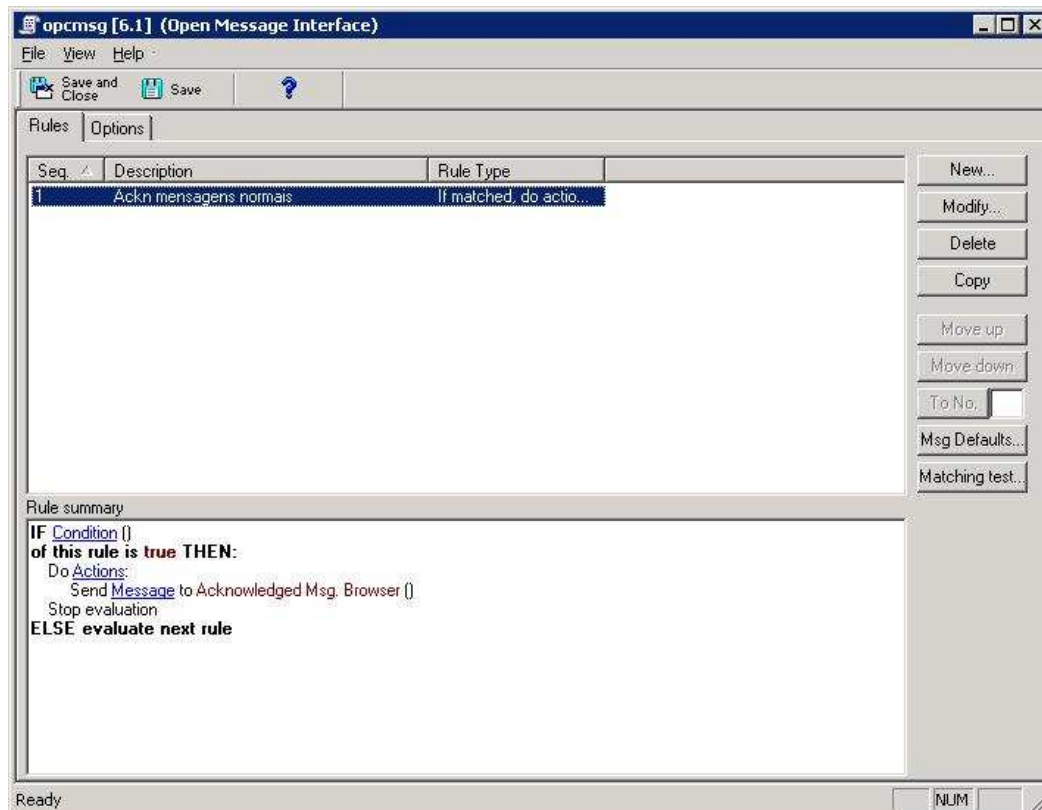



Figura 3.8 - Configurações de política *Open Message Interface*

A mesma politica é também utilizada para evitar a propagação de mensagens indesejadas para níveis superiores de gestão da rede, como o caso da mensagem de se efectuar uma copia de segurança com sucesso, este tipo de mensagens de interesse para uma monitorização diária não são de relevância a nível superiores de gestão onde apenas se esta interessado nas performances e funcionamento das aplicações.

3.2.7. Scheduled Task

Trata-se de uma das mais interessantes políticas de monitorização, podendo a mesma utilizar scripts no seu funcionamento. Esta política cria tarefas programadas em cada equipamento, tarefas que podem ir de efectuar cópias de segurança, verificação de aplicações até á limpeza de ficheiros periodicamente para libertar espaço na unidade lógica (Figura 3.9).

Uma tarefa agendada poderá mesmo enviar mensagens pelos agentes ao operador informando-o de ocorrências na execução dos *scripts*. A implementação encontrada na EDP contém as mais variadas tarefas, na maioria dos equipamentos efectuando monitorização de processos gerando mensagens de anomalias na arvore de serviços aquando da falha dos processos monitorizados.

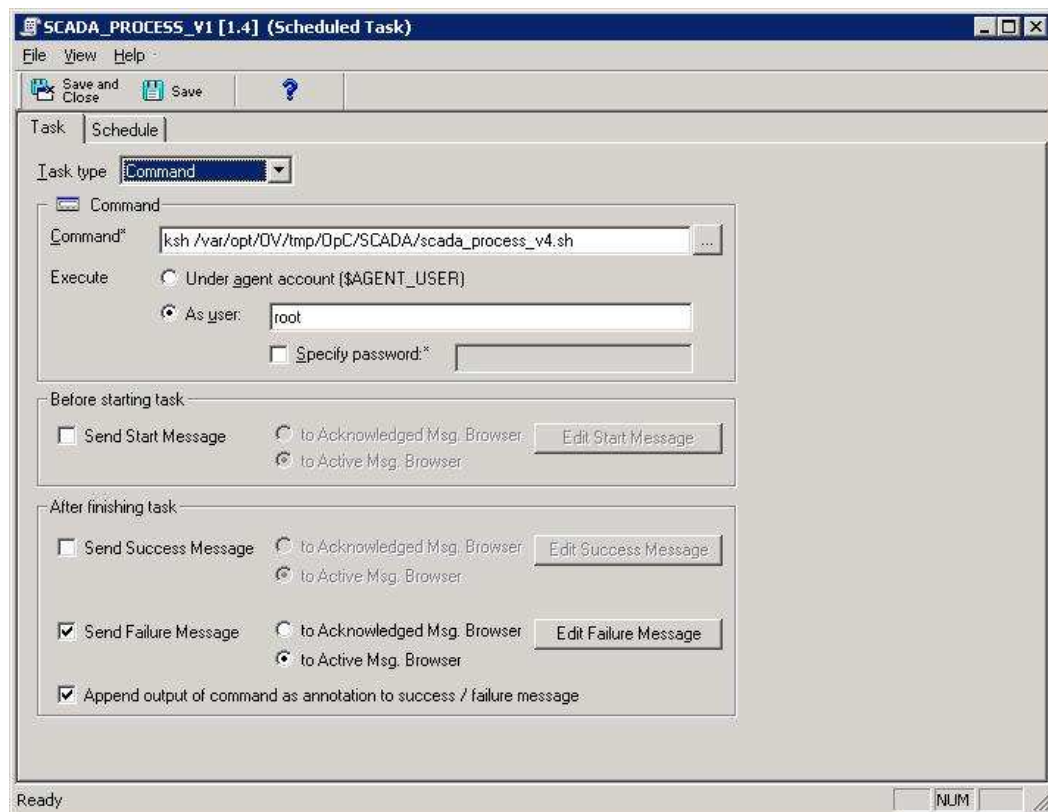



Figura 3.9 - Configurações de política *Scheduled Task*

3.2.8. Service Auto-Discovery

Trata-se não de uma política mas sim de uma das ferramentas do HP-OpenView (Figura 3.10), esta ferramenta é vocacionada para quando colocada no agente, inspeccionando todos os programas existentes no equipamento e envia através de um algoritmo de reconhecimento mensagens de anomalias aquando das aplicações detectadas alterarem o seu estado de funcionamento.

Trata-se de uma forma de determinação de anomalias muito pouco versátil e ampla, não detectando um grande número de acontecimentos, a mesma é aconselhada apenas na descoberta de novos equipamentos de rede quando estes comunicam com um equipamento já monitorizado.

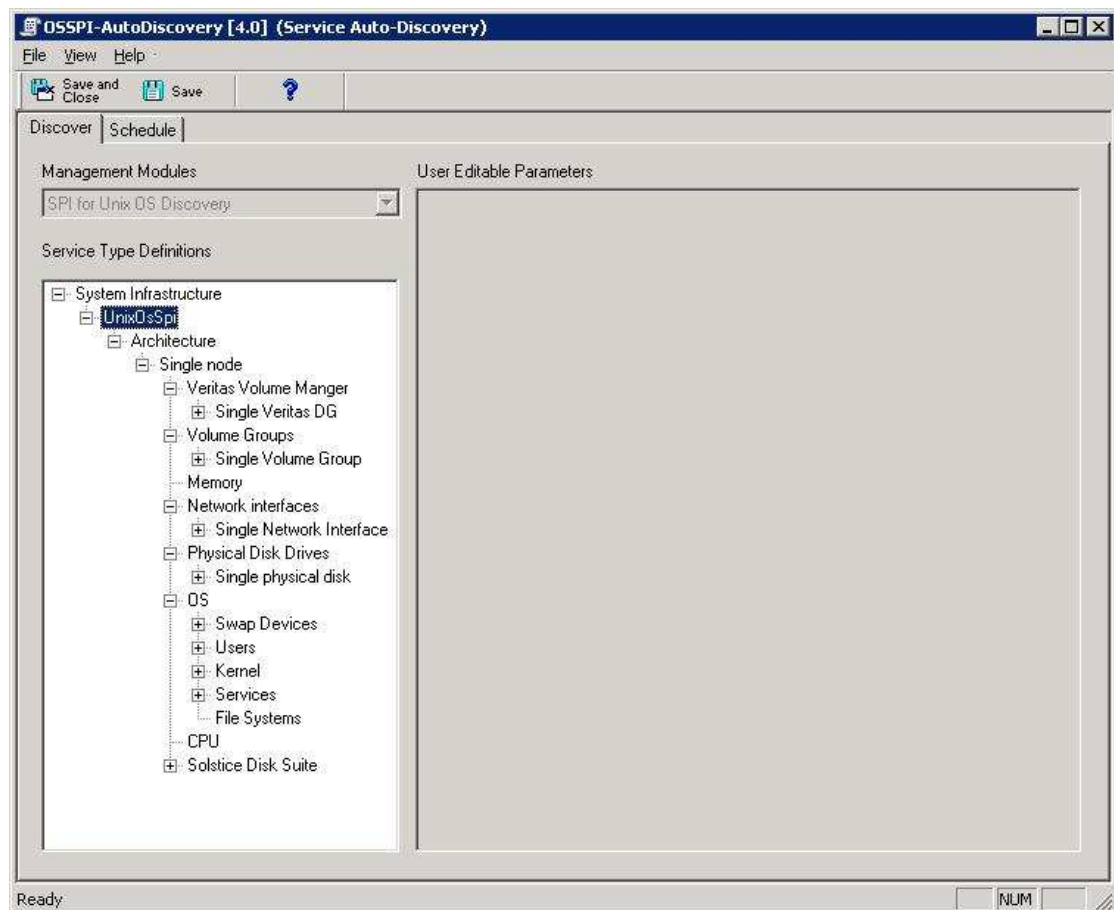



Figura 3.10 - Configurações de política *Service Auto-Discovery*

3.2.9. Service/Process Monitoring

Estas políticas têm o poder de monitorizar aplicações com vários processos, a mesma determina o estado actuar de cada processo, se activo, inactivo, em execução ou parado e avisa o operador aquando de uma anomalia detectada.

As regras de monitorização de cada processo baseiam-se no número de processos a detectar podendo uma aplicação ter várias instâncias do mesmo processo, bem como a detecção de processos indesejados (Figura 3.11).

A detecção de processos indesejados acontece quando se tem com antecedência a informação da implementação de uma aplicação, e sabendo-se que quando determinado processo é executado então a aplicação detectou uma anomalia e está a entrar em modo de segurança, trata-se de um procedimento normal em aplicações de segurança ou de risco eminente para com pessoas e bens.

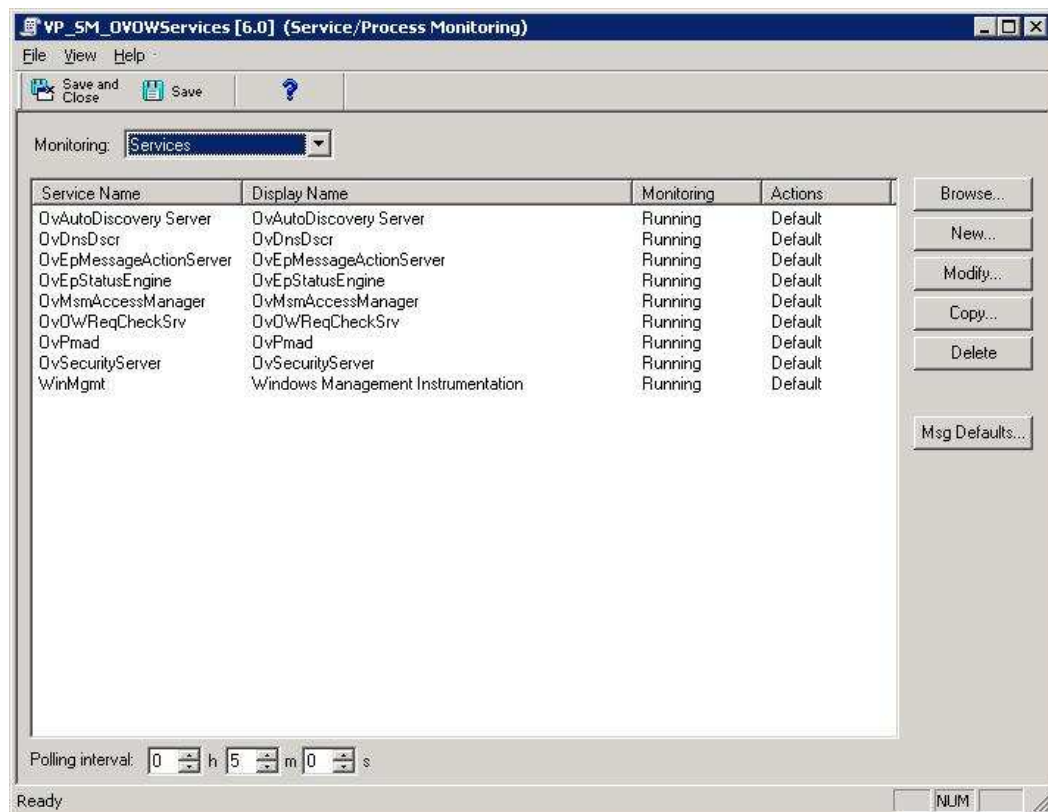



Figura 3.11 - Configurações de política *Service/Process Monitoring*

3.2.10. SNMP Interceptor

Esta política esta preparada para a monitorização de mensagens SNMP e a geração de mensagens para o operador aquando da detecção de uma ou mais anomalias. Neste caso mensagens contendo erros, portas de equipamentos fechadas ou em recusa de acesso, detecção e monitorização de equipamentos de baixo nível como é o caso de *routers*, impressoras e outros equipamentos com capacidade de comunicação por protocolo SNMP (Figura 3.12).

A existência da mesma necessita da instalação do NNM que efectua a monitorização de tramas SNMP.

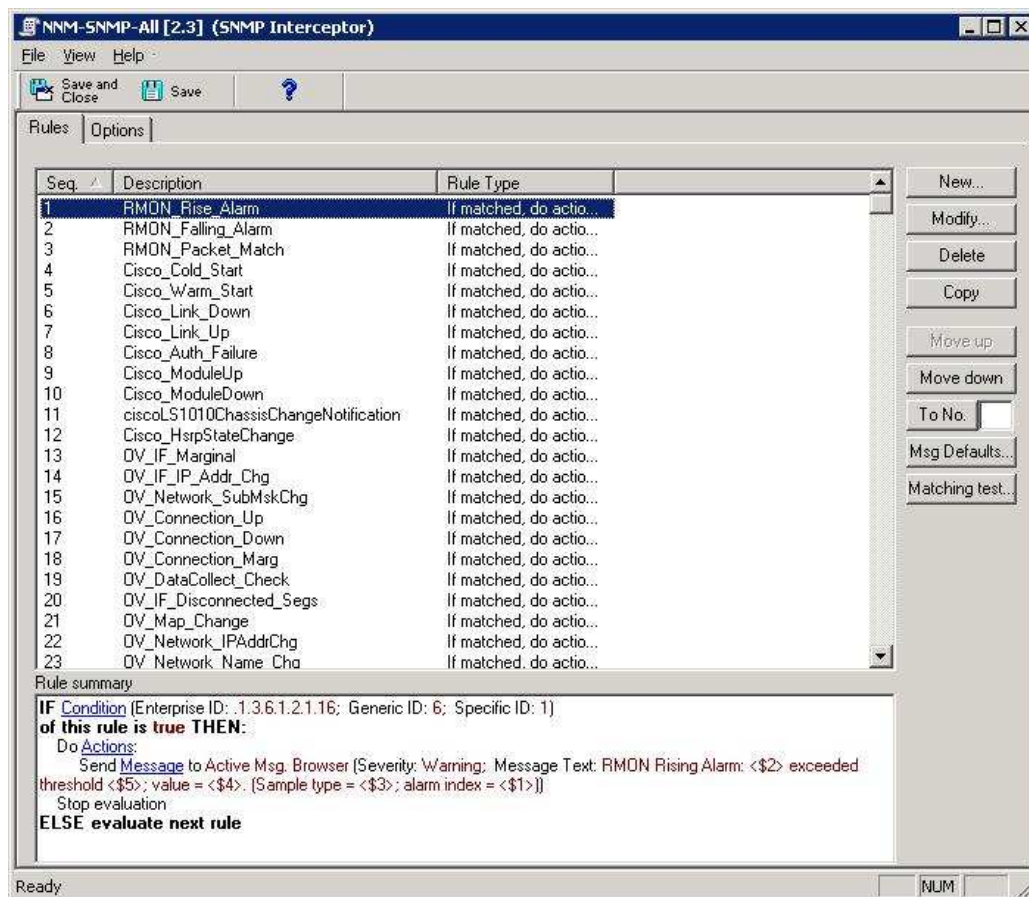



Figura 3.12 - Configurações de política *SNMP Interceptor*

3.2.11. Windows Event Log

Trata-se da política de monitorização os registos de anomalias presentes no sistema operativo Microsoft Windows (Figura 3.13), nestes registos passíveis de serem consultados pelo Painel de controlo \ Ferramentas Administrativas, encontram-se grandes quantidades de informação útil sobre o desempenho do sistema operativo, bem como de ferramentas e aplicações da Microsoft. Sendo então de um elevado interesse a monitorização e filtragem de mensagens geradas nos mesmos, esta política permite facilmente escolher que tipos de mensagens contidas nestes registos são relevantes e o envio da informação das mesmas ao operador. É ainda interessante reparar que estes ficheiros não registam apenas acontecimentos directos, registando também ordens de execução, acessos e o término de processos tendo este sido de uma forma premeditada ou anómala.

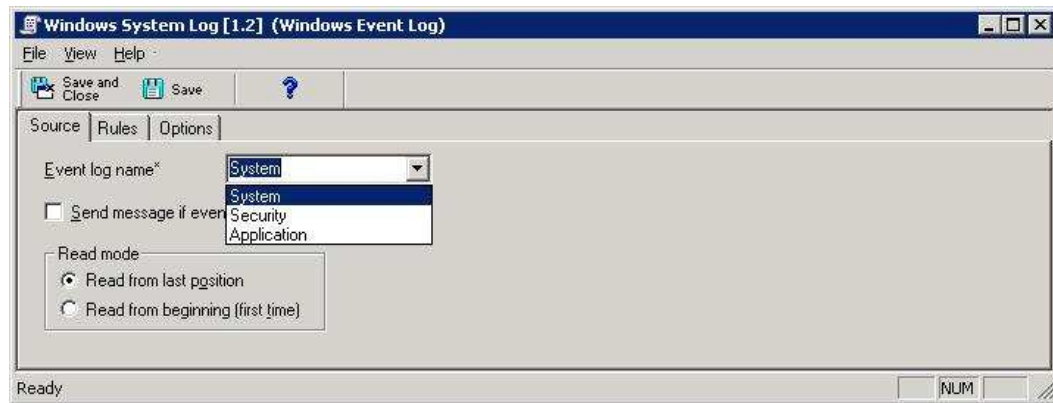



Figura 3.13 - Configurações de política *Windows Event Log*

3.2.12. Windows Managment Interface

Trata-se de uma política internamente ligada á ferramenta da Microsoft WMI, proporcionando uma monitorização das classes constantes nesta mesma. Estas subdividem-se em classes de instancias e de eventos, sendo as mesmas monitorizadas por regras que determinam o aparecimento de um novo evento, bem como a criação e finalização de uma instancia (Figura 3.14).

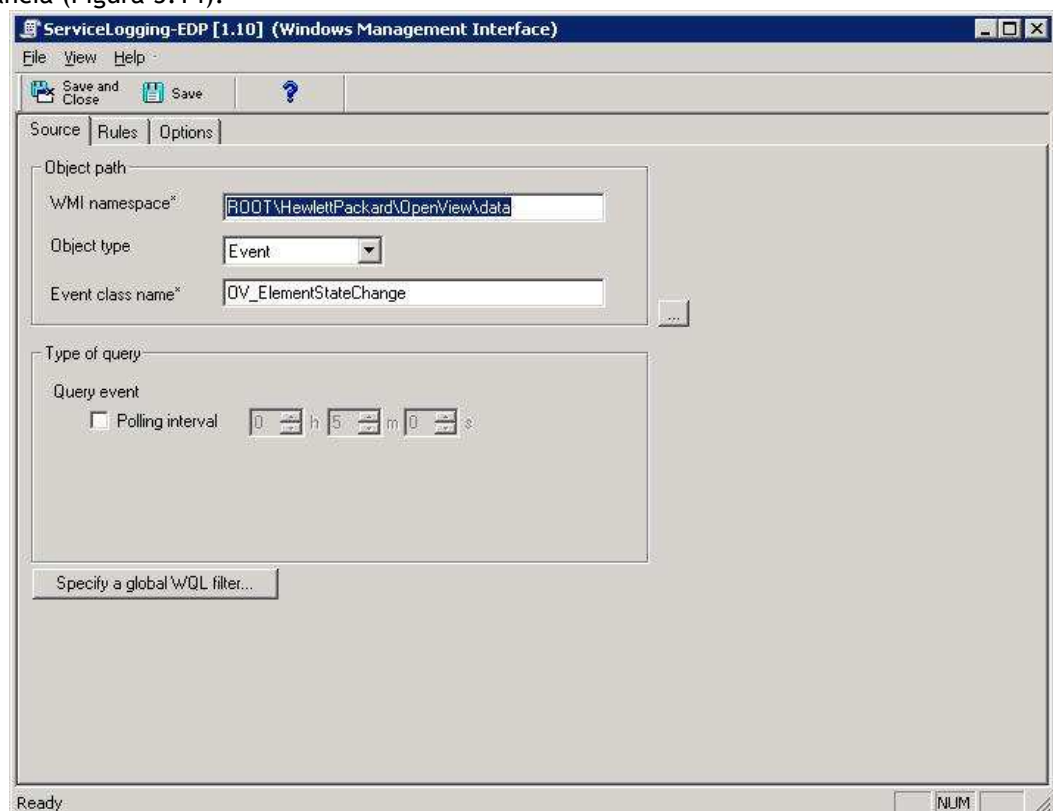



Figura 3.14 - Configurações de política *Windows Management Interface*

3.3. Mensagens

Nas políticas de monitorização foi muitas vezes referido que a quando da identificação de uma anormalidade esta informaria o operador, tal comunicação é efectuada por meio de mensagens. Estas mensagens são estruturadas da mesma forma para todas as políticas, apenas identificando a política por meio de um campo associado.

As mensagens enviadas ao operador não se limitam a aparecer no ecrã de monitorização, as mesmas encontram-se divididas em níveis de gravidade, para o mesmo estabelecer prioridades de análise e reparação. Por vezes estas mensagens implementam informações colocadas aquando da criação da política, medidas a serem tomadas pelo operador para a reparação da anomalia bem como uma lista de algumas ferramentas que solucionam a avaria ou de monitorização para obtenção de mais informação sobre a mesma (Figura 3.15 á esquerda).

As mensagens possuem um parâmetro de configuração (Figura 3.15 á direita) que identifica o seu estado. Estados que poderão ser *unacknowledge*, quando uma mensagem é enviada ao operador com um problema necessitando de uma intervenção do mesmo ou apenas para informação, *acknowladge* quando uma mensagem não tem informação útil para a situação actual mas que é relevante de registo, sendo as mensagens estruturadas com este parâmetro não são dispostas ao operador passando directamente para as mensagens antigas, *auto-acknowladge*, quando se trata do fim de uma anomalia e as mensagens que se encontram no operador já não são verdadeiras, estas são enviadas automaticamente para o registo de histórico, isto deve-se à recepção de uma mensagem que identifica este procedimento.

Existem ainda associadas a estas a opção de *owner* a qual permite a um operador identificar que se encontra a resolver a anomalia, trata-se de uma opção muito útil no caso de existirem dois ou mais operadores de rede, possibilitando a estes darem conhecimentos aos outros que já se encontram a investigar e reparar a anomalia que produziu a mensagem inicial.

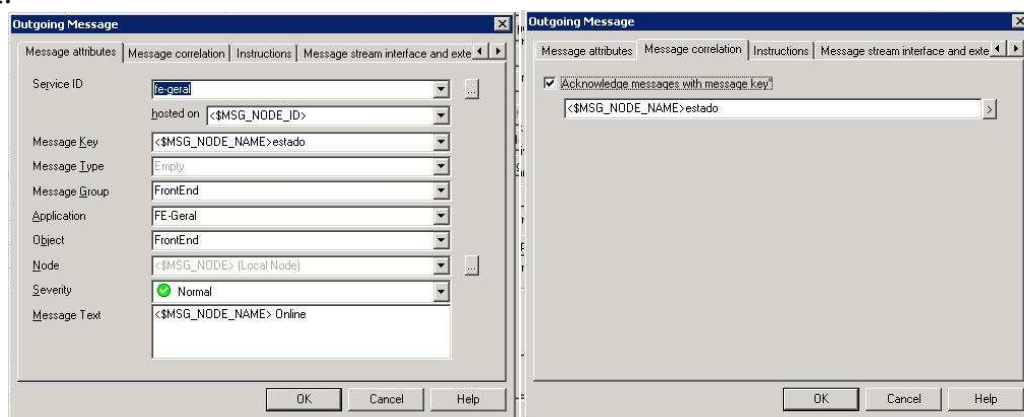



Figura 3.15 – Configuração das mensagens enviadas ao operador

3.4. Ferramentas

A solução HP-OpenView de gestão centralizada de equipamentos não efectua apenas a monitorização dos mais diversos equipamentos, esta também pode interferir no decorrer do seu funcionamento, iniciar aplicações, efectuar actualizações de software e muito mais.

Fazendo uso do agente do HP-OpenView de onde este para além da geração das mensagens a enviar ao operador, pode também preceder a execução de scripts.

Scripts que são invocados para execução, remotamente pelo operador na consola de comando do HP-OpenView, de uma forma cíclica colocando-se os mesmos a serem executados nas politicas '*Scheduled Task*', ou a serem executados a quando da geração de mensagens de anomalia.

Esta última opção é das mais úteis pois proporciona que ao ser detectada uma anomalia na execução de uma aplicação, a mesma mensagem poderá executar um script onde termina a execução da aplicação e inicia a numa nova instancia isto decorrendo em questões de minutos e de onde muitas das vezes o utilizador final nem consegue observar a queda do serviço.

Estas ferramentas encontram-se não só ligadas às mensagens geradas como também podem ser activadas em todas os equipamentos, equipamentos com funcionalidades específicas, ou mesmo num único equipamento. Sendo as ferramentas executadas por ordem do operador para identificação e comprovação do funcionamento, observando-se que neste caso os resultados e mensagens gerados pela execução da ferramenta serão enviados para a consola do operador podendo este ver e analisar esta informação.

3.5. Árvore de Nós

A árvore dos nós é criada tendo em consideração a estruturação interna das redes existentes (Figura 3.16), onde o HP-OpenView irá funcionar obtendo-se assim uma imagem constante das redes o que proporciona uma melhor interpretação e percepção da localização dos equipamentos, bem como de uma rápida intervenção na estrutura de IT em caso de anomalia, avaria ou actualização.

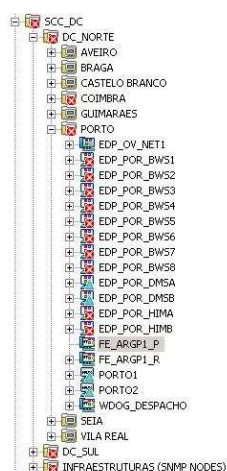



Figura 3.16 - Árvore de nós

Figura 3.17 – Lista de mensagens

Esta árvore (Figura 3.16) fornece uma separação dos equipamentos por área geográfica o que subdivide a análise de anomalias apenas a uma área possibilitando o isolamento a um dado ponto não afectando o serviço global.

Ao percorrer a árvore de Nós facilmente o operador se apercebe do seu funcionamento bem como este poderá facilmente ver os equipamentos contidos em cada uma das redes existentes.

A mesma apresenta uma representação da mensagens sob a forma tabelar (Figura 3.17) de onde se pode identificar facilmente o processo, hardware ou variável do sistema que se encontra com anomalia.

3.6. Árvore de serviços

A árvore de serviços tem uma estrutura semelhante á dos nós (Figura 3.18), estando está mais vocacionada à recepção de mensagens destinadas a serviços, nesta árvore podemos encontrar não equipamentos mas serviços que os mesmos fornecem.

A árvore de serviços encontra-se dividida por aplicações. Na sua extensão podemos identificar a dependência para com os serviços globais, permite observar a subdivisão das aplicações em cada área geográfica e a sua dependência do sistema operativo e hardware.

Genericamente esta estrutura pode ser observada como uma ramificação em árvore ou mesmo em forma de mensagens que afectam o devido sector, ou aplicação podendo-se direccionar meios especializados com a aplicação ou hardware em anomalia.

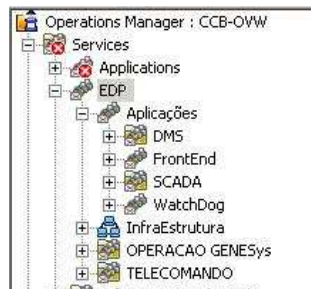



Figura 3.18 - Árvore de serviços

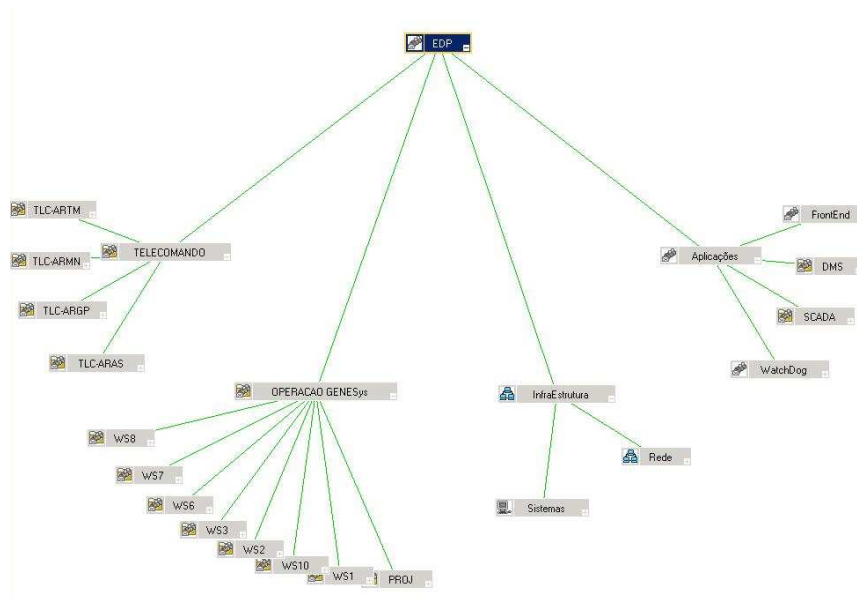



Figura 3.19 - Mensagens estruturadas em árvore de serviços

Esta forma de estruturação permite ainda uma navegação mais do ponto de vista da gestão de IT (Figura 3.19), abstraindo-se nos níveis superiores de mensagens irrelevantes sendo apenas de realce o aparecimento perante o operador de rede de mensagens que afectem o serviço e não os componentes de execução paralela.

De fácil observação são também as dependências das várias aplicações de onde estas contribuem para o funcionamento da estrutura. Com a analise de dependências facilmente se observa o que aconteceria se uma dada aplicação e ou processo terminasse a sua execução, podendo-se desta forma identificar pontos de estrangulamento e tomar medidas de manutenção ou redundância para em caso de anomalia se garantir a estabilidade do sistema.

Para que uma mensagem afecte a árvore de serviços, a mesma terá que se encontrar parametrizada para tal. Na criação do serviço a ser monitorizado existe a possibilidade de associar o mesmo a várias e diferentes mensagens bem como as fórmulas de cálculo com base nessas mensagens, estas apenas afectam o serviço quando uma ou mais mensagens críticas são detectadas ou apenas quando existir queda total ou parcial do mesmo.

Esta implementação é valida também para ramos superiores da árvore existindo regras de propagação na mesma com base nas mensagens anexas ao serviço e no seu número.

3.7. Pacotes

A criação de pacotes implementa uma organização centralizada das políticas existentes, estas podem ser aglomeradas em listas. Este agrupamento é encarado como uma ajuda na medida em que se pode criar pacotes para monitorização de serviços e de equipamentos, bem como os dois em simultâneo, sendo posteriormente mais cómodo a instalação das políticas em novos equipamentos, abstraindo-se o operador de procurar as políticas específicas e as colocar em cada um dos novos equipamentos, tendo-se em conta que estas se encontram no referido pacote bastará instalar o mesmo no equipamento e ficam totalmente configuradas para operações de monitorização.

Capítulo 4

Caracterização das políticas e ferramentas

No Inicio deste estudo já se encontravam implementadas na empresa EDP várias políticas de monitorização, sendo muitas destas políticas padronizadas. Ou seja, já se encontravam pré definidas na aplicação base, as mesmas foram criadas por técnicos da HP uma vez que são usadas repetidas vezes em quase todos os seus clientes sendo necessária apenas a identificação dos equipamentos a monitorizar pela mesma.

O HP-OpenView possuía também políticas implementadas por funcionários da EDP e empresas subcontratadas para optimização e gestão da plataforma. As políticas então implementadas encontram-se a efectuar a monitorização de um grande número de parâmetros nas máquinas, sendo especialmente focadas na vigilância de aplicações específicas da empresa e tendo impacto na operacionalidade da aplicação e para com o fornecimento do serviço.

Na realização deste trabalho todas estas políticas existentes previamente no HP-OpenView foram estudas, de forma a avaliar a sua funcionalidade na actual estrutura de rede, tendo-se encontrado casos que as mesmas não se adequam, e procedendo-se ao desenvolvimento de políticas e em alguns casos implementado se novas regras.

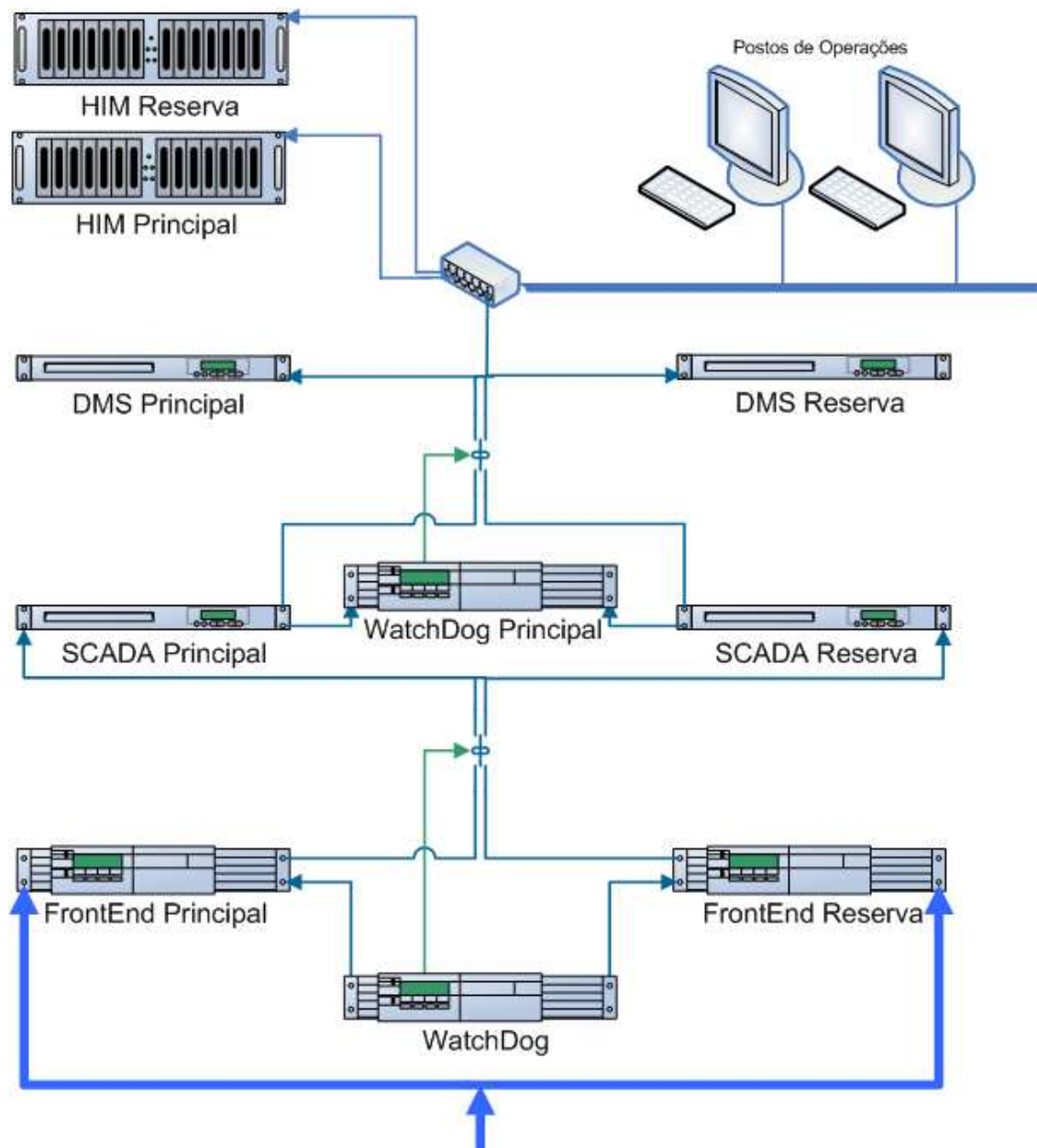



Figura 4.1 - Esquema de rede

A rede de comunicações entre servidores da EDP tem uma estrutura vertical tal como representada na Figura 4.1. Estes servidores recebem a informação através de maquinas de entrada chamados FrontEnd's. Os FrontEnd's são computadores adaptados cada um com 22 portas série as quais recebem dados das subestações pelos protocolos proprietários IEC, CETT, PUR, EDP, TG809 e 4F, com os dados recebidos, estes equipamentos efectuam a sua conversão e adaptação para tramas TCP/IP, transferindo a informação para os servidores SCADA.

Ao efectuar uma monitorização contínua do processamento efectuado pelos FrontEnd's encontram-se os WatchDog's, equipamentos em muito parecidos com os FrontEnd's, sendo que estes se diferenciam pela inexistência das portas série de entrada. Os WatchDog's têm

como função a comutação de equipamentos de entrada, isto devido á existente duplicação de equipamentos, um WatchDog em funcionamento comunica com o FrontEnd em utilização efectuando testes, para determinação da necessidade de comutação. Os WatchDog's podem ainda ser comandados remotamente possibilitando a comutação manual de FrontEnd's.

De entre o núcleo de servidores utilizados pela EDP á que destacar duas das máquinas nucleares para que o sistema GENESys funcione correctamente, trata-se do SCADA e da DMS. Sendo que os servidores SCADA encontram-se monitorizados por um WatchDog que efectua a comutação entre os dois existentes em cada centro de despacho, as DMS por seu lado não têm a necessidade da existência de um WatchDog efectuando a monitorização uma da outra directamente e assumindo o controlo a DMS de reserva aquando necessário.

O servidor SCADA, têm como base o sistema operativo HP-UX 10 de elevada performance e fiabilidade, possibilitando assim uma grande estabilidade e confiança nos serviços disponibilizados pelo equipamento, sendo que no decorrer deste trabalho apenas tive conhecimento de um reinício das referidas máquinas sendo que o mesmo fora provocado no decurso de uma actualização pela empresa EFACEC. Estes equipamentos são responsáveis por:

- Tratamento da informação recebida;
- Registo de eventos nas bases de dados de históricos;
- Recepção de ordens do operador e transmissão das mesmas aos dispositivos;
- Criação de uma listagem de alarmes.

As máquinas DMS estão a executar um sistema operativo Microsoft Windows, como suporte às aplicações do GENESys. Sendo que as aplicações em execução na mesma efectuam a ligação entre o processamento SCADA e o controlador da rede, nesta ligação as DMS efectuam a ligação das variáveis a objectos gráficos de fácil compreensão e monitorização, providenciando um ambiente de trabalho gráfico (Figura 2.1) de onde um engenheiro pode facilmente observar a rede existente de uma forma mais intuitiva.

Na lista de equipamentos constantes nos servidores podemos ainda encontrar os equipamentos HIM, máquinas desenvolvidas para alojar uma base de dados Oracle com a finalidade de registarem todos as eventos da rede, trata-se do registo providenciado pelos servidores SCADA, no decorrer das suas operações. Este equipamento não sendo vital para o serviço prestado pela empresa, proporciona uma avaliação das medidas tomadas por operadores e do seu impacto nos serviços, tendo a sua relevância quando se pretende avaliar e estudar acontecimentos para futuros estudos.

Do lado oposto aos servidores existentes situam-se as BWS (*Blade Working Station*) e WS (*Working Station*), sendo que as WS são um interface directo para com o utilizador estando a aplicação gráfica a ser executada directamente e contendo ligações de rede directamente para com os servidores SCADA, DMS e HIM em serviço. As BWS são *blades* de um armário servidor composto por processadores ITANIUM, de onde se subdivide o poder de processamento para emular vários equipamentos, sendo que estes equipamentos são acedidos

de uma forma remota por HP-RemoteGrafics, do lado do utilizador existe um equipamento de menor capacidade a executar uma versão de Linux dedicado a HP-RemoteGrafics, desta forma efectua-se neste tipo de máquinas um isolamento da rede de comunicação entre os servidores e o utilizador. A existência das máquinas com ligações directas aos servidores deve-se apenas como mais um método de redundância para garantir que se o referido núcleo falhar ainda existe estes equipamentos para se efectuar a gestão da rede.

4.1. Politicas de monitorização dos agentes

Estas políticas destinam-se a monitorização do bom funcionamento do agente, encontrando-se na base dos mesmos e instaladas juntamente com os respectivos agentes. Encontram-se nomeadamente a serem executadas no servidor central e têm como ponto de partida, vários factores de performance tais como, o tempo de resposta dos agentes, a operacionalidade e o volume de informação gerada por este.

As também estão presentes na própria máquina a ser monitorizada, criando ficheiros de registos onde guardam tudo o que ocorre com o agente, nomeadamente mensagens de execução que são guardadas em ficheiros próprios.

4.2. Ficheiros de registos

O interesse da descrição e estudo destes ficheiros é devido á sua monitorização em futuras implementações e a informação relevante contida nos mesmos.

4.2.1. Do agente

4.2.1.1. Registo de configurações 'ConfigFile policy package for Windows Nodes.log'

Neste ficheiro de registo é possível encontrar as configurações do agente, bem como um registo das ocorrências a quando da instalação do mesmo.

A sua alteração irá provocar na existência de um reinício do agente de alteração de configurações, podendo o agente ser programado e alteradas definições a partir da edição directa deste ficheiro.

4.2.1.2. Registos do JavaAgent

Este ficheiro de registos é criado em todos os equipamentos a onde se tenha instalado o agente.

Nele é registada toda a actividade de sincronização com o HP-OpenView Operations, erros de ligações entre os dois, e existência de possíveis tarefas a executar periodicamente.

Aquando de uma sincronização, o agente inicia a transmissão do histórico para o *Operation*, e no final da sincronização este confirma os dados enviados e termina. De notar que este histórico é apagado do agente no final desta operação.

Este processo repete-se periodicamente de 24 em 24 horas.

Esta é uma forma de garantir que nenhuma mensagem é perdida.

4.2.1.3. Registo das comunicações entre o agente o servidor Operation 'OvSvcDiscAgt.log'

Neste ficheiro são encontrados os registos de ocorrências entre o servidor HP-OpenView Operations e o agente local.

```
[Wed Apr 08 02:00:09 2009][169:353] clientPipes:124 WaitNamedPipe FAILED
\\.\pipe\OvCpexIn GetLastError = 121, The semaphore timeout period has expired.
```

Figura 4.2 - Extracto de uma anomalia no 'OvSvcDiscAgt.log'

No exemplo da Figura 4.2 podemos ver um erro de ligação por *pipe*, de onde o mesmo servidor se encontrava com excesso de trabalho e recusou a ligação do agente ficando a mesma agendada para um período posterior.

4.2.1.4. Registo de limpeza de base de dados 'coda.log'

Um dos eventos agendados pelo núcleo do HP-OpenView trata-se da eliminação semanal de registos.

Nesta execução é eliminado o ficheiro existente mais antigo, criando-se um novo. Este processo segue uma lógica numérica, de onde os referidos ficheiros mais antigos têm o menor número tendo o mais recente um número superior.

4.2.1.5. Registo de erros do agente opcmona 'opcerror'

Neste ficheiro estão guardadas as mensagens geradas pelo processo '*opcmona*' *(*agente de comunicação para com o servidor*)*, o qual regista erros na execução das políticas aplicadas ao

nó. Este regista ainda os pedidos de reinício de processos e de publicação de mensagens, pelo utilizador.

4.2.2. Ficheiro de registo Event Log do Microsoft Windows

O ficheiro do Windows *Event Log* regista a ocorrência de anomalias geradas pelos mais diversos serviços e aplicações, não sendo estas aplicações apenas do sistema operativo, podendo o mesmo conter informações de anomalias de outras aplicações como é o caso de antivírus, e ferramentas que recorram aos comandos 'EVENTCREATE', 'EVENTQUERY' e 'EVENTTRIGGERS', os quais permitem a geração de mensagens nos registos de eventos do Windows, a listagem das mesmas permite a análise de ocorrências por parte do sistema operativo, exemplo, o fecho imprevisto de uma aplicação monitorizada por um *trigger*, será registada uma nova entrada no ficheiro de eventos contendo informação da aplicação e o erro retornado pela mesma.

4.3. Politicas Gerais

4.3.1. Sistemas operativos Microsoft Windows

Tabela 4.1 — Definições das políticas de monitorização de hardware em Microsoft Windows

Designação	Tipologia	Mensagens geradas	Variável a ser monitorizada	Intervalo de inspecção
Políticas estudadas				
OvSvcDiscErrorLog	Logfile Entry	Aviso Acknowladge	Registo do agente	5 Minutos
WINOSSPI-EventLogService	Measurement Threshold	Conhecimento Acknowladge mensagem anteriormente geradas	Processo 'services'	5 Minutos
WINOSSPI-Net_BytesTotalSec	Measurement Threshold	Crítica acima dos 30.000 bytes/seg	Total bytes/sec	4,53 Minutos

		Aviso 20.000 bytes/seg		
WINOSSPI-Net_CurrentCommands	Measurement Threshold	Crítica acima dos 15comandos/seg Aviso 10comandos/seg	Total comandos/sec	5,07 Minutos
WINOSSPI-Net_NetworkErrorsSec	Measurement Threshold	Crítica acima dos 2erros/seg Aviso 1 erro/seg	Total erros/sec	4,52 Minutos
WINOSSPI-Net_ReadsDeniedSec	Measurement Threshold	Crítica acima dos 2recusas/seg Aviso 1 recusa/seg	Total recusas/sec	5,08 Minutos
WINOSSPI-OS_FwdApplicationWarnError	Windows Event Log	Crítica Aviso	Event Log ID=1018 e ID=1017, origem =”Perfilib”	
WINOSSPI-PlugnPlayService	Measurement Threshold	Imformação	Dispositivos nas portas USB	5,01 Minutos
Políticas alteradas				
WINOSSPI-CpuBottleneck_NT4 WINOSSPI-CpuBottleneck_Win2k	Measurement Threshold	Aviso critico activo Acknowladge mensagem anteriormente geradas	TotalCpuTime TotalCpuTime TotalCpuTime InterruptTime	5 Minutos
WINOSSPI-DiskBottleneck_NT4 WINOSSPI-DiskBottleneck_Win2k	Measurement Threshold	Aviso critico activo Acknowladge mensagem anteriormente geradas	DiskTime DiskQueueLenght AvgDiskSecTransfer	5 Minutos
opcmsg	Open Message Interface	Normal Acknowledge	Mensagens normais	
WINOSSPI-RPCService-NT WINOSSPI-RPCService-Win2k	Measurement Threshold	Aviso serviço em pausa	Serviços, RPC	5,02 Minutos

		Crítica serviço parou		
WINOSSPI-SysMon_AvgDiskSecTransfer	Measurement Threshold	Alarmante de maior que 3 Crítica se maior que 5	Discos lógicos	4,51 Minutos
WINOSSPI-SysMon_DiskBusyCheck	Measurement Threshold	Alarmante Crítica	Discos lógicos	10 Minutos
WINOSSPI-SysMon_DiskFullCheck	Measurement Threshold	Crítica Space	Discos lógicos	8 Minutos
WINOSSPI-SysMon_CpuSpikeCheck-NT4 WINOSSPI-SysMon_CpuSpikeCheck-Win2k	Measurement Threshold	Alarmante Crítica	Processador	2,58 Minutos
WINOSSPI-SysMon_PageFileCheck	Measurement Threshold	Crítica	Paging File	7 Minutos
Políticas implementadas				
Chk_Reboot	Measurement Threshold	Normal Acknowledge		
Filtro mensagens internas	Open Message Interface		Internal	

4.3.1.1. Política que monitoriza o reiniciar do sistema ‘Chk_Reboot’

A existência de uma política que monitorize e registe todas as instâncias em que uma máquina reinicia é de especial interesse para a manutenção uma vez que o reinício poderá corrigir grande parte dos erros existentes no equipamento. Também é relevante em termos estatísticos, de onde se pode ter o interesse em se saber o número médio de horas de execução contínua.

Esta politica, efectua uma medição com um *polling* de 5 minutos do contador de sistema. A quando da detecção do mesmo com um tempo inferior a 900 segundos a mesma anuncia uma mensagem de nível normal com auto *acknowledge* da referida ocorrência de reinicio.

4.3.1.2. Politica de filtragem das mensagens internas

Esta politica foi criada para filtrar as mensagens geradas pelo agente ‘opcmona’, colocando as mensagens de menor gravidade diga-se normais directamente como acknowledge, não sendo o operador de rede confrontado com elevadas quantidades de informação e apenas observando as mensagens que realmente produzem informação fulcral para a manutenção do sistema.

A mesma política segue uma regra de comparação de mensagens, Open Message, de onde se define as regras para as mensagens que iram ser enviadas ao servidor HP-OpenView Operations e as que apenas ser enviadas directamente para o registo de históricos.

De uma forma construtiva foram então observadas, que apenas se teria interesse na observação das mensagens geradas internamente, com os vários níveis de impacto sobre o sistema. Sendo as mensagens geradas pelo agente ‘opcmona’ ocultas e consideradas como irrelevantes para o manutenção do sistema no seu normal desempenho.

Estas mensagens do ‘opcmona’, devem-se ao facto da existência de tempos limites para execução prévia de uma dada política ou pequeno programa, sendo gerada uma mensagem de aviso em caso da ultrapassagem deste mesmo tempo, bem como de em muitos equipamentos existirem várias ocorrências da mesma política, estas devem-se a comutação de servidores HP-OpenView do Porto para Lisboa.

De reparar que no seu estado actual esta política não se encontra a efectuar o pretendido, sendo este motivo um dos objectos de estudo posterior deste trabalho (5.1. Mensagens Internas).

4.3.1.3. Politica de acknowledge das mensagens normais ‘opcmsg’

Sendo o HP-OpenView uma interface para com o operador/ supervisor de sistema, este mesmo, não necessita de ter ao seu dispor todas as mensagens geradas pelos agentes.

Desta conclusão, nota-se que é apenas de interesse para com o utilizador as mensagens de grau superior ao normal, sendo as restantes relevantes apenas para registo na base de dados e posterior analise.

Como tal existe uma politica de filtragem de mensagens. A mesma política, dedica-se exclusivamente a observação das mensagens normais e proceder ao seu *acknowledge*. De notar que existem mensagens que não serão filtradas, nomeadamente as de reinício de um equipamento. Estas mensagens de reinício são importantes para o operador pois este poderá partir de uma situação de limpeza de anteriores erros, procedendo ao *acknowledge* de mensagens anteriores ao referido reinício.

A mesma política efectua um filtro a procura de mensagens produzidas pelos agentes com um grau Normal e efectua o referido *acknowledge* das mesmas.

Esta política é executada no agente local sendo as mensagens enviadas para o OpenView Operations já configuradas como *acknowledge*.

4.3.1.4. Política de erros do agente ‘OvSvcDiscErrorLog’

Esta tarefa tem como objectivo a inspecção do ficheiro de registo do agente, ficheiro este já documentado acima no ponto (4.2.1.3), de onde se lê o ficheiro a partir da última leitura efectuada, verificando a existência de novas linha, neste caso mensagens de anomalias. Se as mesmas existirem e fizerem parte da lista seguinte esta regra emite uma mensagem de aviso para a pasta de mensagens ‘*Acknowladged*’, este processo inicialmente enviaria as mensagens para a pasta ‘*Active Messages*’, facto que se veio a constatar irrelevante, de pouco interesse uma vez que as mesmas não reflectem o estado do sistema, apenas o estado dos agentes, adicionando por isso informação não relevante para o controlo e manutenção da rede.

4.3.1.5. Política que detecta reduções nas performances do sistema ‘WINOSSPI-CpuBottleneck_NT4’ e ‘WINOSSPI-CpuBottleneck_Win2k’

Estas políticas estão apenas separadas pela forma como as suas variáveis são acedidas, sendo que as duas têm o mesmo objectivo.

A medição do estrangulamento e a baixa nas performances das máquinas onde se encontram colocadas, como tal estas efectuam a observação das variáveis:

Variável	Componente	Aviso no valor	Descrição
TotalCpuTime	Processor Queue Length	2	Número de *threads* em espera
TotalCpuTime	CPU Utilization Percentage	90	Percentagem de uso do processador
TotalCpuTime	Total Number os CPDs on the system		Número de processadores em uso
InterruptTime	Percentage Interrupt Time	60	Tempo que o processador despende a atender interrupções de hardware

Pressupõem-se então que o sistema irá gerar uma mensagem avisando o operador se:

- o *TotalCpuTime* exceder a percentagem máxima, definida pelo operador;
- se *ProcQueueLen* for maior que o máximo predefinido por processador, TotalCPUs;
- se InterruptTime for maior que o máximo definido;

Este gera ainda uma mensagem de erro no caso de:

- TotalCpuTime for maior que o valor máximo definido e (TotalCpuTime maior ou igual ao TotalCPUs somado com o máximo de *Queue Length* por processador, ou o InterruptTime for maior ou igual ao seu valor máximo definido)

A sua implementação tem como base VB-Script sendo os valores das variáveis passadas ao script por apontadores.

Quando a situação regressar a sua normalidade, descida para valores novamente aceitáveis é gerada uma mensagem de *auto-acknowledge* a qual envia para o histórico as mensagem previamente geradas por esta política.

4.3.1.6. Política que detecta estrangulamentos no acesso ao disco 'WINOSSPI-DiskBottleneck_NT4' e 'WINOSSPI-DiskBottleneck_Win2k'

Esta política monitoriza possíveis estrangulamentos no acesso ao disco através da análise das seguintes variáveis:

Variável	Componente	Aviso no valor	Descrição
DiskTime	% Disk Busy Time	66	Número de *threads* em espera
DiskQueueLenght	Disk Queue Lenght	2	
AvgDiskSecTransfer	Average Disk Sec/Transfer	0.3	

Este script implementado em VB-script tem como estrutura a geração de mensagens se:

- DiskTime maior ou igual ao limite máximo definido e DiskQueueLenght maior que o seu limite máximo definido;
- AvgDiskSecTransfer maior que o limite definido.

Esta análise é efectuada a cada 5 minutos, sendo que as mensagens de erros a quando da reposição á normalidade serão acknowledge para histórico.

4.3.1.7. Política que verifica se o registo de serviços do Windows se encontram em execução 'WINOSSPI-EventLogService'

A política verifica a existência dos serviços do Windows que são responsáveis pela gestão de várias aplicações, protocolos, registos de anomalias entre outras funcionalidades existentes durante o funcionamento do sistema operativo.

Para tal esta politica serve-se da aplicação 'opcntprocs.exe' que faz parte do HP-OpenView Agente, para determinar se o processo '*services*' do sistema operativo Microsoft

Windows se encontra em execução. Bem como do batch script ‘opcntservice_chk.bat’ para verificar em que estado se encontra o serviço.

Com a informação destes dois processos de monitorização, e com a ajuda de um VB-script, o HP-OpenView verifica se é a primeira vez que este script é executado, sendo necessário a criação de uma lista inicial de serviços em execução. Caso contrario este fará uma comparação do actual estado dos serviços com a listagem de serviços preexistentes, alertando o utilizador a quando da alteração no estado de um destes ou do conjunto.

4.3.1.8. Política monitoriza os discos dos equipamentos ‘WINOSSPI-LogicalDisk_NT4_Logging’ e ‘WINOSSPI-LogicalDisk_Win2k_Logging’

Estas regras de monitorização inspeccionam todas as variáveis do disco com o objectivo de determinar o estado de acesso ao disco, espaço disponível e tempos médios de escrita e de leitura.

Para tal serve-se das variáveis de sistema:

Variável
LogicalDisk % Disk Read Time
LogicalDisk % Disk Write Time
LogicalDisk % Free Space
LogicalDisk Avg. Disk Queue Length
LogicalDisk Avg. Disk sec/Transfer
LogicalDisk Disk Bytes/sec

Estas regras encontram-se inoperacionais estando colocada em todos os equipamentos monitorizados. A mesma não gera qualquer mensagem de aviso ao operador

4.3.1.9. Política que monitoriza estrangulamentos na memoria ‘WINOSSPI-MemoryBottleneck_NT4’ e ‘WINOSSPI-MemoryBottleneck_Win2k’

Para um sistema funcionar devidamente a monitorização continua das performances da memória contida no equipamento é vital, uma vez que a escassez da mesma poderá produzir estrangulamentos, ou seja atrasos no processamento de informação e até mesmo falhas no acesso a mesma informação.

Para a sua monitorização o WMI do Windows dispõe de várias variáveis as quais o HP-OpenView tem acesso:

Variável	Aviso no valor	Descrição
PageFaultRate	9 pages/sec	Acesso a paginas que não estão na memória
AvailableMBytes	4MB	Memória disponível

Para a monitorização da memoria física de um equipamento e uma vez que a mesma não se limitada apenas ao espaço físico que dispõe, podendo partes da mesma estarem armazenadas em disco, as variáveis em questão terão que ter uma grande flexibilidade para não gerarem erros, os quais ao fim de pouco tempo se encontrariam corrigidos pois esta foi completada com o arquivo de paginação em disco.

Como tal esta apenas gerará uma mensagem avisando o operador quando o acontecimento seguinte se repetir 5 vezes no espaço de tempo de 5 minutos:

AvailableMBytes maior que o máximo definido e PageFaultRate maior que o máximo definido.

4.3.1.10. Política que descobre novas aplicações na plataforma Windows 'WINOSSPI-MSWINApp_AutoDiscovery'

O AutoDiscovery é uma das ferramentas implementadas de origem no HP-OpenView, tem como principal objectivo a detecção de novas aplicações nos equipamentos monitorizados. Esta política é executada uma vez a cada 24 horas numa hora predefinida, em grande parte dos equipamentos monitorizados esta é executada as 3:00 horas periodicamente.

De se notar que o resultado da mesma não gera qualquer informação ao operador, registando apenas em ficheiro, os resultados da sua ocorrência. Os ficheiros resultantes da mesma serão analisados por outras politicas se assim necessário.

4.3.1.11. Política que monitoriza alterações no sistema operativo 'WINOSSPI-MSWINSys_AutoDiscovery'

A execução desta política como a anterior efectua-se uma forma cíclica e a uma hora pré-programada, na grande maioria dos equipamentos 3:10 horas, sendo o objectivo da mesma detectar actualizações ou alterações na estrutura do Sistema operativo Microsoft Windows.

Esta inspecciona a instalação de pacotes de segurança, *Service Pack's*, módulos do Windows e alterações nos ficheiros raiz.

4.3.1.12. Política que inspecciona a utilização da rede 'WINOSSPI-Net_BytesTotalSec'

Esta política inspecciona o número de *bytes* enviados e recebidos pela placa de rede durante um segundo, produzindo um erro se a mesma estiver a causar um congestionamento de rede.

Variável	Aviso no valor	Descrição
Bytes Total/sec	20.000	Número de *bytes* transaccionados num segundo
	30.000	

Neste caso considera-se que a placa de rede esta congestionada quando o número de bytes enviados e recebidos num segundo for superior a 20.000 bytes/seg, sendo então geradas mensagens de erro ao operador.

4.3.1.13. Política que monitoriza os comandos enviados 'WINOSSPI-Net_CurrentCommands'

A implementação desta política conta o número de comandos de rede gerados e produzidos pelo equipamento, estes comandos serão: ping, netstat, psexecute, entre outros.

Variável	Aviso no valor	Descrição
Current Commands	10 Gera aviso	Número de comandos por segundo
	15 Gera erro	

Se o número de comandos detectado ao fim de um segundo for superior ao máximo especulado este equipamento emite uma mensagem de aviso ao operados de acordo com o número de comandos a mais a ultrapassar o limite.

4.3.1.14. Política de monitorização de erros na comunicação 'WINOSSPI-Net_NetworkErrorsSec'

Esta política monitoriza o número de erros por segundo gerados na tentativa de comunicação, ou seja o número de pacotes falhados por segundo, permitindo ao utilizador verificar o estado da conexão de rede bem como o estado dos dados que enviou.

Um elevado número de erros de transmissão, poderá significar a falha na transmissão de dados, e o aparecimento de ficheiros e informações corrompidas.

Variável	Aviso no valor	Descrição
Network Errors/sec	1 Gera aviso	Número erros de transmissão por segundo
	2 Gera erro	

4.3.1.15. Política de monitorização de recusa na ligação 'WINOSSPI-Net_ReadsDeniedSec'

Politica que monitoriza a recusa de ligação pelo servidor de um determinado ponto de rede.

O aparecimento de um evento deste género implica que o equipamento se encontra extremamente ocupado, sendo a recusa de ligação um pressuposto ao aparecimento de erros, ou uma consequência do aparecimento de algum erro.

Variável	Aviso no valor	Descrição
Reads Denied/sec	1 Gera aviso	Tentativas de comunicação fachadas por segundo
	2 Gera erro	

Esta política emite mensagens de anomalia a quando da recusa de um ou mais pedidos de ligação, isto foi definido com o valor mínimo uma vez que se considera que cada ligação é importante e traz informação vital para o bom desempenho do sistema.

4.3.1.16. Política que monitoriza as bibliotecas de performance de sistema operativos Microsoft 'WINOSSPI-OS_FwdApplicationWarnError'

A monitorização destas bibliotecas encontra-se associada a chave de registos 'HKEY_LOCAL_MACHINESoftwareMicrosoftWindows NTCurrentVersionPerflib' a qual funcionando como apontador, identifica a localização e os dados contidos nas bibliotecas, estas bibliotecas permitem a obtenção de elementos de performance usados noutras políticas, para a monitorização de processador, memória, disco, e dos mais variados equipamentos associados ao equipamento como um todo.

Para a determinação de anomalias o Windows no seu funcionamento regista as anomalias destas bibliotecas nos ficheiros de 'EventLog' os quais são inspeccionados pela política procurando o código 1018 associado a este tipo de eventos, fazendo transparecer mensagens com o ID=1018 para o operador.

4.3.1.17. Política de monitorização de dispositivos 'Plug and Play', ' WINOSSPI-PlugnPlayService'

Esta política inspecciona a introdução de um novo dispositivo, no equipamento. Sendo de extrema importância em redes fechadas, pois detecta possíveis tentativas de intrusão ao se introduzir elementos estranhos e de possível contagio no sistema. Embora esta política não tenha um grande impacto na monitorização em tempo real da rede esta poderá evitar

problemas futuros ao advertir o operador para possíveis entradas de agentes externos na rede.

Variável	Aviso no valor	Descrição
Services.exe	1	Inspecciona os serviços do Windows
Plug_and_play	1	Inspecciona a componente dos serviços

Para a monitorização destas variáveis, o agente serve-se da aplicação 'opcntprocs.exe', para determinar se o processo '*services*' do sistema operativo Microsoft Windows se encontra em execução.

Bem como do batch script 'opcntservice_chk.bat' para verificar em que estado se encontra o serviço 'Plug_and_play' e as suas componentes internas, retornando o número de dispositivos conectados por este método as portas USB do equipamento.

4.3.1.18. Política que identifica o serviço de eventos externos 'WINOSSPI-RPCService-NT4' e 'WINOSSPI-RPCService-Win2k'

O serviço de RPC (*Remote Procedure Call)* é um dos serviços nucleares na monitorização e controlo da ferramenta HP-OpenView, sendo este serviço usado para a comunicação de comandos, actualização de políticas, envio de ordens de gestão e execução de ferramentas associadas a plataforma.

Este serviço possibilita a conexão por linha de comandos ao equipamento, o que com o auxílio das *Power Tools* PS da Microsoft, traz o controlo de componentes do sistema para outro nível, não sendo necessário aceder por *RemoteDesktop*, usando esta ferramenta pudesse executar as mais vaiadas operações sem que o actual utilizador do equipamento note ou mesmo detecte a intrusão efectuada.

Este serviço do Microsoft Windows bem pois possibilitar o controlo remoto de equipamentos que até a data era necessário a autorização do utilizador para se aceder aos mesmos, tendo este utilizador que parar o seu trabalho a quando do tempo de manutenção.

Esta política apenas monitoriza a disponibilidade deste serviço alertando para a sua inactivação.

Variável	Aviso no valor	Descrição
Services.exe	1	Inspecciona os serviços do Windows
RPC	1	Inspecciona a componente dos serviços

No seu funcionamento esta serve-se da aplicação 'opcntprocs.exe' que faz parte do HP-OpenView Agente, para determinar se o processo 'services' do sistema operativo Microsoft Windows se encontra em execução. Bem como do *batch* script 'opcntservice_chk.bat' para verificar em que estado se encontra o serviço.

4.3.1.19. Política que monitoriza a velocidade do disco rígido 'WINOSSPI-SysMon_AvgDiskSecTransfer'

A monitorização desta variável deve-se ao facto de a mesmas indicar possíveis atrasos na execução de aplicações, isto devido a incapacidade de leitura e escrita de informação no disco lógico.

Como tal e com a analise das performances dos discos usados foi restringido um valor máximo bastante inferior ao limite físico de forma a evitar previamente este tipo de questões, ora por melhorando as performances passando para um nível RAID, ora por subdividindo as aplicações e os acessos ao disco para outros equipamentos.

Variável	Aviso no valor	Descrição
Avg. Disk sec/transfer	3%,5%	Media de tempo de transferência de dados com o disco

4.3.1.20. Política que inspecciona a utilização do disco 'WINOSSPI-SysMon_DiskBusyCheck'

Esta política observa a utilização do disco, uma vez que um excesso de uso na escrita e leitura do mesmo operam levar a um degradação do mesmo e a perda de informação. Como tal observa-se a progressão de duas variáveis de forma a determinar e evitar o uso contínuo.

Variável	Aviso no valor	Descrição
Avg. Disk Queue Lenght	5%,10%	Media de tempo em espera de escrita ou leitura
Disk Time	60%, 80%	Tempo de utilização do disco

De se notar que a mesma politica apenas é executada uma vez a cada 10 minutos sendo desprezada a informação entre este intervalo de tempo nesta análise é apenas utilizando uma amostragem das variáveis de sistema.

4.3.1.21. Politica que monitoriza o espaço livre em disco 'WINOSSPI-SysMon_DiskFullCheck'

A criação desta política teve como base a determinação da percentagem do espaço livre em disco, no seu cálculo é pois lida a capacidade da unidade e comparada esta informação com o espaço ocupado no mesmo, obtendo assim uma medida de utilização do disco.

Trata-se de uma política importante na determinação de discos lotados em servidores, o que poderá acontecer inesperadamente com o acumular de dados não previstos, isto é de externa importância pois uma vez que num disco lotado podendo existir perdas de informação.

4.3.1.22. Politica que inspecciona sobrecargas no processador 'WINOSSPI-SysMon_CpuSpikeCheck-NT4' e 'WINOSSPI-SysMon_CpuSpikeCheck-Win2k'

Trata-se de uma monitorização de longo prazo preventiva e que poderá levar a decisão de actualizar o equipamento antes que este entre em sobrecarga e não consiga processar a informação em tempo útil.

Para a determinação das mensagens são monitorizadas as seguintes variáveis:

Variável	Aviso no valor	Descrição
Total Privileged Time		Tempo de processos com maior privilégios
Total User Time	80%,90%	Tempo de utilização processador por parte do utilizador
Total Processor Time		Tempo de funcionamento do processador

4.3.1.23. Política que monitoriza o arquivo de 'Paging File' do Windows 'WINOSSPI-SysMon_PageFileCheck'

Esta detecção da expansão no ficheiro do *paging* é normalmente usada para libertar para o disco blocos de memória menos activa, é relevante no ponto em que um ficheiro de *paging* demasiado grande poderá levar a uma lentidão e arrasto do sistema, pois este terá que ler a informação do disco para a memória para efectuar o processamento da mesma. Logo a melhor solução seria mesmo o menor valor possível para este ficheiro, como tal não é possível efectua-se uma monitorização para determinar o ponto onde o sistema é de tal forma lento que poderá gerar problemas nos sistemas subsequentes.

Variável	Aviso no valor	Descrição
Paging File Use	>=80%	Percentagem de utilização do ficheiro de memoria do disco

4.3.1.24. 'WINOSSPI-WINOS_NT4_Logging' e 'WINOSSPI-WINOS_Win2k_Logging'

Esta ferramenta não esta relacionada com a criação de mensagens, mas sim com o registo de variáveis de ambiente para utilização posterior na criação de gráficos, relatórios e análises estatísticas.

4.3.1.25. RemoteDesktop

Trata-se de uma ferramenta desenvolvida com o objectivo de se efectuar uma ligação aos equipamentos usando as ferramentas da Microsoft RemoteDesktop, com a mesma pode-se efectuara a manutenção directa em caso de anomalia ao equipamento, podendo a mesma ferramenta ser chamada de uma mensagem de anomalia do Agente, para uma rápida reparação ou comutação para outros equipamentos.

Esta ferramenta está limitada e apenas funciona em ambientes Windows XP, 2000 e 2003 Server.

4.3.1.26. VNC

Trata-se de uma ferramenta muito parecida com a anterior invocando a aplicação VNC no ponto onde a anterior invocava a aplicação da Microsoft RemoteDesktop. O VNC é uma aplicação proprietária que permite efectuar o controlo a equipamentos remotos, muito parecida com o RemoteDesktop, mas esta podendo ser executada em ambientes Microsoft Windows NT4.0. Esta aplicação VNC tem grandes desvantagens em relação ao RemoteDesktop, nomeadamente a velocidade e qualidade na interface disponibilizada.

4.3.1.27. NetMeeting

Trata-se de mais uma ferramenta de monitorização e controlo equivalente as duas já apresentadas anteriormente. Esta pode se encontrada em ambientes Microsoft Windows e foi antecessora do RemoteDesktop, tal como a aplicação VPN esta também apresenta um interface de baixa qualidade e com uma operação muito lenta dando a noção de arrasto na gestão de aplicações.

4.3.1.28. Restart

Esta trata-se da uma das mais perigosas ferramentas implementadas no decurso desta dissertação, a mesma faz uso do comando PSshutdown para forçar o reinício do equipamento.

Esta ferramenta foi pois programada para encerramentos de forma crítica, não deixando tempo de enceramento dos processos e obrigando os mesmos a parar de uma forma rápida.

4.4. Politicas de monitorização de processos específicos

4.4.1. FrontEnd's

Como facilmente se entende existindo duas máquinas a executar uma aplicação com a mesma finalidade, o seu software interno terá que ser diferente de acordo com o seu estado perante a execução do serviço. Sendo que perante o restante conjunto de mecanismos estas são observadas como se de apenas uma se tratasse.

Os *FrontEnd's* encontram-se então um em execução fornecendo todos os dados para as restantes aplicações e o seu homologo a executar alguns processos chave caso seja preciso um arranque rápido do mesmo. Este comando de arranque parte de um *WatchDog* que decide com base num algoritmos de falhas o melhor equipamento para a realização desta tarefa.

Os processos existentes em cada FrontEnd podem divergir, na medida em que os FrontEnd's dependem dos protocolos de comunicação não sendo necessário a monitorização de protocolos que o FrontEnd não esteja a utilizar, como pode ser observado na Tabela 4.2.

Tabela 4.2 — Protocolos de comunicação associados a cada FrontEnd

		Protocolo					
		IEC	CETT	PUR	EDP	TG809	4F
Equipamentos	FE CC AVE E SOUSA	X	X	X	X		
	FE CC AVEIRO	X	X	X			
	FE CC BEJA	X		X			X
	FE1 CC CARENQUE	X		X			X
	FE1 CC CARENQUE			X			
	FE CC CASTELO BRANCO	X	X	X			X
	FE CC COIMBRA	X	X	X			
	FE CC LEIRIA		X	X			
	FE CC LOULÉ	X		X		X	
	FE CC LOURES	X		X			X
	FE CC MINHO	X		X	X		
	FE1 CC OLHO BOI	X		X			X
	FE2 CC OLHO BOI	X		X			X
	FE1 CC PALHAVÃ	X		X			X
	FE2 CC PALHAVÃ	X		X			X
	FE2 CC PALHAVÃ	X		X			X
	FE CC PORTO	X		X	X		
	FE CC S. SEBASTIÃO	X		X		X	
	FE CC SEIA	X	X	X			
	FE CC TRÁS-OS-MONTES	X		X	X		

Políticas instaladas nos agentes de cada FrontEnd.

Tabela 4.3 — Definições das políticas de monitorização do Sistema GENESys para FrontEnd's

Designação	Tipologia	Mensagens geradas	Variável a ser monitorizada	Intervalo de inspecção
Políticas estudadas				
FEbackground	Measurement Threshold	Normal auto acknowledge Crítica Activa	Processos	1 Minuto
FEcontrolsMFE	Measurement Threshold	Normal auto acknowledge Crítica Activa	Processos	1 Minuto
FEcronos	Measurement Threshold	Normal auto acknowledge Crítica Activa	Processos	1 Minuto
FEdbinit	Measurement Threshold	Normal auto acknowledge Crítica Activa	Processos	1 Minuto
FEedp_app	Measurement Threshold	Normal auto acknowledge Crítica Activa	Processos	1 Minuto
FEfrontendMFE	Measurement Threshold	Normal auto acknowledge Crítica Activa	Processos	1 Minuto
FEiec870_app	Measurement Threshold	Normal auto acknowledge Crítica Activa	Processos	1 Minuto
FEiec870_llc	Measurement Threshold	Normal auto acknowledge Crítica Activa	Processos	1 Minuto
FEpurapp	Measurement Threshold	Normal auto acknowledge Crítica Activa	Processos	1 Minuto
FEpurllc	Measurement Threshold	Normal auto acknowledge Crítica Activa	Processos	1 Minuto
FEservices	Measurement Threshold	Normal auto acknowledge Crítica Activa	Processos	1 Minuto
FEsuper	Measurement Threshold	Normal auto acknowledge Crítica Activa	Processos	1 Minuto
FEtrace	Measurement Threshold	Normal auto acknowledge Crítica Activa	Processos	1 Minuto
FEttags	Measurement Threshold	Normal auto acknowledge Crítica Activa	Processos	1 Minuto
FEwatchdogMFE	Measurement Threshold	Normal auto acknowledge Crítica Activa	Processos	1 Minuto
nc	Measurement Threshold	Normal auto acknowledge Alarmante Activa	Processos	1 Minuto

Políticas implementadas				
FE_StandBy	Logfile Entry	Normal Online Normal Standby	FEmemdbg Users	4 Minutos

4.4.1.1. Verifica se o FrontEnd se encontra operacional como Online ou HotStandBy

Nesta política implementa a monitorização de um ficheiro lendo o conteúdo do ficheiro sempre da primeira posição, com o valor lido e por uma regra de comparação, o mesmo determina o estado actual do "FrontEnd".

Esta politica está associada a duas mensagens, se FrontEnd online emite uma mensagem normal auto *acknowledge*, se HotStandBy emite uma mensagem normal auto *acknowledge*, ambas contendo uma designação do estado 'FrontEnd Online', 'FrontEnd *StandBy*'.

```
c:\HPOpenview\estado2.txt
  users = 00800000H          server = (0021) A ON, B OFF
```

Esta política não se encontra em funcionamento devido a não interligação entre os scripts e o programa FEmemdbg. Este caso será abordado mais para a frente no decorrer deste trabalho.

4.4.1.2. Processo FEbackground

A monitorização deste processo é efectuada pela função do HP-OpenView 'opcntprocs.exe' que lista os processos em execução, seguindo-se a comparação do resultado da mesma.

4.4.1.3. Processo FEcontrolsMFE

Este processo é responsável pelos controlos do FrontEnd. Comandos verificados e alterados pelo SCADA central a quando necessário ajustes ou existência de alguma ocorrência anómala.

4.4.1.4. Processo FEcronos

Processo de contadores do sistema, este efectua a contagem dos dados recebidos e enviados para prevenir perdas de informação.

4.4.1.5. Processo FEdbinit

Processo de ligação a base de dados, neste caso a uma base de dados Oracle presente na máquina HIMA e HIMB

4.4.1.6. Processo FEedp_app

Processo que efectua a ligação entre o FrontEnd e os computadores industriais, em que é utilizado o protocolo de comunicação proprietário EDP.

4.4.1.7. Processo FEfrontendMFE

Este processo efectua a alteração do estado do FrontEnd de Online para HotStandBy, a quando de uma ordem do WatchDog, e ou operador, para a execução do mesmo.

4.4.1.8. Processo FEiec870_app

Processo que efectua a ligação entre o FrontEnd e os computadores industriais, em que é utilizado o protocolo de comunicação proprietário IEC870.

4.4.1.9. Processo FEiec870_llc

Este processo encontra-se internamente ligado ao anterior FEiec870_llc, sendo necessário a existência dos dois para um normal funcionamento da comunicação.

4.4.1.10. Processo FEpurapp

Processo que efectua a ligação entre o FrontEnd e os computadores industriais, em que é utilizado o protocolo de comunicação proprietário PUR.

4.4.1.11. Processo FEpurllc

Este processo encontra-se internamente ligado ao anterior FEpuradd, sendo necessário a existência dos dois para um normal funcionamento da comunicação.

4.4.1.12. Processo FEscan_hdlc

Processo que efectua a ligação entre o FrontEnd e os computadores industriais, em que é utilizado o protocolo de comunicação proprietário HDLC.

4.4.1.13. Processo FEservices

Não me foi possível averiguar as funcionalidades deste processo, existindo apenas uma informação por parte da EFACEC de que o mesmo é crucial e de elevada importância para o normal funcionamento do sistema.

4.4.1.14. Processo FEsuper

Processo que efectua a supervisão de todo o FrontEnd emitindo avisos e efectuando registos de anomalias existentes neste equipamento FrontEnd.

4.4.1.15. Processo FEtrace

O processo trace (Figura 4.3), efectua a codificação e monitorização de todas as tramas, recebidas e enviadas, pelas portas do FrontEnd, sendo as mensagens observadas no seu normal funcionamento.

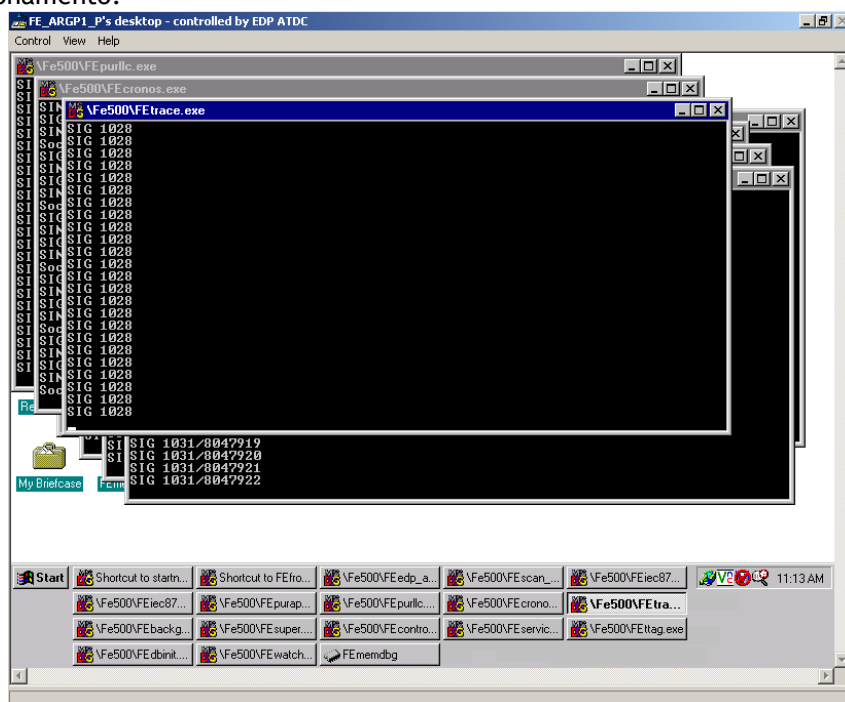



Figura 4.3 – Shell de monitorização do processo FEtrace

4.4.1.16. Processo FEttags

Este processo efectua a ligação dos dados recebidos para com as *tags* (variáveis) do sistema SCADA global.

4.4.1.17. Processo FEwatchdogMFE

Este processo efectua a comunicação entre o FrontEnd e o WatchDog, Permitindo assim assegurar uma rápida comutação de processos entre os dois FrontEnd's.

4.4.1.18. Processo nc

Comando que permite o WatchDog efectuar a comutação, a sua relevância não é relativamente crítica para o normal funcionamento do sistema, sendo apenas utilizada pelo WatchDog para efectuar uma comutação.

4.4.1.19. Processo reinício de FrontEnd

Trata-se de uma ferramenta desenvolvida para efectuar o lançamento dos processos do FrontEnd sem reiniciar o equipamento. Esta ferramenta acede ao processo dos FrontEnd's FEfrontendMFE.exe enviando-lhe o comando 'k', o qual é interpretado pelo mesmo processo como uma ordem de reinício.

4.4.2. WatchDog

O WatchDog é um equipamento em muito parecido com os próprios FrontEnd's, este apenas não dispões das ligações de entrada para se ligar aos computadores industriais presentes nas subestações e postos de transformação.

Têm então como função inspeccionar se os valores da máquina que actualmente se encontra definida como online são querentes, se o tempo de resposta em polling situa-se na margem de segurança previamente definida, ou mesmo se o processo esta em execução. Isto deve-se a execução de um processo desenhado no sistema que envia informação directamente do FrontEnd para o WatchDog, possibilitando ao WatchDog com está informação o cálculo dos seus algoritmos e a tomada de decisão. Enviando no caso de ser necessário efectuar uma comutação de equipamentos, um sinal a relés externos aos equipamentos, sendo que estes relés procedem a inactivação da unidade e á comutação do FrontEnd de recurso para o modo online. A mesma máquina voltara a estar operacional após o restar ordenado, entrando em modo HotStandBy.

Tabela 4.4 — Definições das políticas de monitorização do Sistema GENESys para WatchDog's

Designação	Tipologia	Mensagens geradas	Variável a ser monitorizada	Intervalo de inspecção
Políticas estudadas				
FEbackground	Measurement Threshold	Normal auto acknowledge Crítica Activa	Processos	1 Minuto
FEcontrolsMFE	Measurement Threshold	Normal auto acknowledge Crítica Activa	Processos	1 Minuto
FEcronos	Measurement Threshold	Normal auto acknowledge Crítica Activa	Processos	1 Minuto
FEdbinit	Measurement Threshold	Normal auto acknowledge Crítica Activa	Processos	1 Minuto
FEfrontendMFE	Measurement Threshold	Normal auto acknowledge Crítica Activa	Processos	1 Minuto
FEservices	Measurement Threshold	Normal auto acknowledge Crítica Activa	Processos	1 Minuto
FEsuper	Measurement Threshold	Normal auto acknowledge Crítica Activa	Processos	1 Minuto
FEtrace	Measurement Threshold	Normal auto acknowledge Crítica Activa	Processos	1 Minuto
FEttags	Measurement Threshold	Normal auto acknowledge Crítica Activa	Processos	1 Minuto
FEwatchdogMFE	Measurement Threshold	Normal auto acknowledge Crítica Activa	Processos	1 Minuto
nc	Measurement Threshold	Normal auto acknowledge Alarmante Activa	Processos	1 Minuto

4.4.3. SCADA

Estas máquinas são o núcleo central de todo o sistema de monitorização e controlo remoto que garante a continuidade das operações, sendo as mesmas responsáveis pela recolha de informação dos FrontEnd's, o tratamento e disponibilização da mesma informação para bases de dados (HIM), processadores de informação (DMS) e portos de operações (BWS).

As mesmas máquinas correm sobre um sistema operativo de alta fiabilidade em comparação com o seu homólogo Windows instalado na rede, HP-UX, dando o mesmo suporte á execução de vários processos tanto do software de controlo GENESys, como das bases de dados Oracle.

Do ponto de vista de monitorização e controle de processos estes equipamentos são inspeccionados gerando dois tipos de mensagens, as mensagens de processos que reportam anomalias nos processos em execução de acordo com documentos da EFACEC, e mensagens de serviços as quais são geradas por um script agendado que verifica com base em duas lista de processo o estado actual do equipamento, se este se encontra em serviço ou em reserva, sendo gerada uma mensagem para os serviços desta situação bem como provocando mensagem de anomalia no caso de o mesmo equipamento não se encontrar em nenhum destes dois estados.

Tendo em conta a análise de serviços e após um estudo do algoritmo implementado para a sua realização, veio-se a notar a existência de um ficheiro associado ao algoritmo que era periodicamente incrementado com a informação de cada estado. Para um servidor de alto desempenho e ao qual se exigem tempo de resposta muito curto, a existência deste ficheiro punha em causa alocação de memoria todas as vezes que o script era executado, espaço em disco, pois este já tinha um tamanho aceitável de 300MBytes. Com este panorama optou-se pela limpeza deste género de ficheiros para valores controláveis e aceitáveis, este script e descrito no Capítulo 7.

Como a monitorização é efectuada por uma tarefa *Scheduled*, a mesma apenas emite uma mensagem de auto-acknoladge a quando da situação regularizada, ou seja todos os processos detectados em funcionamento.

Tabela 4.5 - Processos SCADA Online

Processo	Nº de Processos	Mensagem	Serviço
Políticas estudadas			
alarm_gateway	2	Crítica	GENESys
alarm_switch	1	Maior	SCATEX
alarms	3	Maior	SCATEX
application_server	2	Crítica	GENESys
arc	3	Maior	SCATEX
cntMULTFE	1	Crítica	SCATEX
db_channel	2	Crítica	GENESys
ddb_mng	1	Crítica	SCATEX
deriv	1	Maior	SCATEX
extreq_ser	1	Crítica	SCATEX

gptim	1	Maior	SCATEX
inifeMULTFE	1	Crítica	SCATEX
navigator	1	Crítica	GENESys
node_manager	2	Crítica	GENESys
ora_d000_despacho	1	Crítica	DB
ora_s000_despacho	1	Crítica	DB
ora_reco_despacho	1	Crítica	DB
ora_smon_despacho	1	Crítica	DB
ora_ckpt_despacho	1	Crítica	DB
ora_lgwr_despacho	1	Crítica	DB
ora_dbw0_despacho	1	Crítica	DB
ora_pmon_despacho	1	Crítica	DB
proc_check	1	Maior	SCATEX
rtevent_bridge	2	Crítica	GENESys
rwevent_bridge	2	Crítica	GENESys
sinc	1	Crítica	SCATEX
slowUpdMem	1	Crítica	SCATEX
supMULTFE	1	Crítica	SCATEX
sx_alrmng_gw	2	Crítica	GENESys
sx_control_gw	2	Crítica	GENESys
sx_login_gw	2	Crítica	GENESys
sx_scada_gw	2	Crítica	GENESys
sx_scheduler	1	Maior	SCATEX
sx_server	1	Crítica	SCATEX
sxservicesMULTFE	3	Crítica	SCATEX
tnslsnr	1	Crítica	DB
ttagMULTFE	1	Crítica	SCATEX
ttagupddb	1	Crítica	SCATEX
updtot_on	1	Crítica	SCATEX
wdogMULTFE	1	Crítica	SCATEX
x_mapping_manager	2	Crítica	GENESys
xterm_check	1	Maior	SCATEX
Políticas implementadas			
java	1	Crítica	GENESys

Tabela 4.6 - Processos SCADA Standby

Processo	Nº de Processos	Mensagem	Serviço
Políticas estudadas			
alarms	3	Maior	SCATEX
arc	1	Maior	SCATEX
cntMULTFE	1	Crítica	SCATEX
ddb_mng	1	Crítica	SCATEX
extreq_ser	1	Crítica	SCATEX
gptim	1	Maior	SCATEX
inifeMULTFE	1	Crítica	SCATEX
navigator	1	Crítica	GENESys
node_manager	2	Crítica	GENESys
ora_d000_despacho	1	Crítica	DB
ora_s000_despacho	1	Crítica	DB
ora_reco_despacho	1	Crítica	DB
ora_smon_despacho	1	Crítica	DB
ora_ckpt_despacho	1	Crítica	DB
ora_lgwr_despacho	1	Crítica	DB
ora_dbw0_despacho	1	Crítica	DB
ora_pmon_despacho	1	Crítica	DB
proc_check	1	Maior	SCATEX
rtevent_bridge	2	Crítica	GENESys
rwevent_bridge	2	Crítica	GENESys
Sinc	1	Crítica	SCATEX
slowUpdMem	1	Crítica	SCATEX
sx_scada_gw	2	Crítica	GENESys
sx_syn_file_transfer_server	2	Maior	GENESys
supMULTFE	1	Crítica	SCATEX
sxservicesMULTFE	2	Crítica	SCATEX
Tnslsnr	1	Crítica	DB
ttagMULTFE	1	Crítica	SCATEX
Ttagupddb	1	Crítica	SCATEX
wdogMULTFE	1	Crítica	SCATEX
x_mapping_manager	2	Crítica	GENESys

Estas políticas foram implementadas e estudadas com base no documento [3], emitido pela EFACEC. Este documento lista os processos considerados críticos e o seu objectivo funcional.

4.4.3.1. Processos SCATEX

Os processos SCATEX descritos na Tabela 4.5 e Tabela 4.57, fazem parte da aplicação antiga de suporte, a qual se encontra actualizada pelo GENESys, aplicação que ainda faz uso destes processos podendo-se utilizar a nova plataforma para se enviar comandos sendo que o GENESys utilizara primeiro os servidores DMS, ou directamente pelos servidores SCADA usando o SCATEX.

4.4.3.2. Processos GENESys

Os processos da aplicação GENESys em execução nos servidores SCADA têm como objectivo a interligação deste servidor com as DMS para a construção gráfica da rede, os mesmos permitem o telecomando e monitorização de todos os actuadores efectuando a interligação de tabelas a uma base de dados grafia contida nas DMS.

4.4.3.3. Processos DB

Na monitorização destes processos será observada a aplicação Oracle que se encontra em execução nesta instância específica do serviço. Sendo que a aplicação Oracle fornece uma base de dados de suporte as estruturas existentes no servidor proporcionando um registo dinâmico dos valores e das variáveis em cada sensor e actuador existente no mundo EDP.

Para além desta função a base de dados proporciona informações a um servidor de histórico HIM o qual armazena todos os eventos que resultam do funcionamento e comando da rede por um período de tempo mais alargado.

4.4.4. DMS

As DMS formam desenvolvidas pela EFACEC na sequência da actualização de SCATEX para GENESys, tendo a sua introdução alterado o esquema de mapeamento tabelar antigamente existente e juntando informação de estruturas gráficas da rede permite a geração do ambiente gráfico que se encontra nos postos de operações. Sendo que no seu funcionamento as DMS processam variáveis geradas pelos servidores SCADA, as alteram para identificação da instalação e do equipamento de onde estas são provenientes, de notar que esta informação da localização das instalações e dos equipamentos se encontra não nas DMS mas sim nos SIT’s

Regionais, sendo que estes equipamentos também têm a função de receberem as informações gráfica de comandos a actuar, identificarem o equipamento e enviam ao SCADA para a execução do referido comando.

Poder-se á dizer que estes equipamentos efectuam a abstracção dos elementos de rede existente, para um ambiente de onde o utilizador apenas necessitara de um conhecimentos de redes energéticas.

De se notar que estes equipamentos são nucleares para o funcionamento da actual aplicação GENESys, passando pelos mesmos toda a informação de controlo, fazendo com que as DMS sejam consideradas como equipamentos de risco muito elevado pois a sua interrupção provoca a paragem no fornecimento de informação ao controlo e do controlo as actuadores.

Tabela 4.7 - Processos DMS

Designação	Tipologia	Mensagens geradas	Variável a ser monitorizada	Intervalo de inspecção
Políticas estudadas				
cim_sync_server-DMS	Measurement Threshold	Normal Online Crítica Activa	Processos	1 Minutos
construction_files_manager-DMS	Measurement Threshold	Normal Online Crítica Activa	Processos	1 Minutos
db_channel-DMS	Measurement Threshold	Normal Online Crítica Activa	Processos	1 Minutos
distributer-DMS	Measurement Threshold	Normal Online Crítica Activa	Processos	1 Minutos
file_manager-DMS	Measurement Threshold	Normal Online Crítica Activa	Processos	1 Minutos
GenerateSynServer-DMS	Measurement Threshold	Normal Online Crítica Activa	Processos	1 Minutos
global_context_manager-DMS	Measurement Threshold	Normal Online Crítica Activa	Processos	1 Minutos
him_wrapper-DMS	Measurement Threshold	Normal Online Crítica Activa	Processos	1 Minutos
ImportSynServer-DMS	Measurement Threshold	Normal Online Crítica Activa	Processos	1 Minutos
java-DMS	Measurement Threshold	Normal Online Crítica Activa	Processos	1 Minutos
local_context_manager-DMS	Measurement	Normal Online	Processos	1 Minutos

	Threshold	Crítica Activa		
Navigator-DMS	Measurement	Normal Online	Processos	1 Minutos
	Threshold	Crítica Activa		
NetState-DMS	Measurement	Normal Online	Processos	1 Minutos
	Threshold	Crítica Activa		
Node_Manager-DMS	Measurement	Normal Online	Processos	1 Minutos
	Threshold	Crítica Activa		
Oracle-DMS	Measurement	Normal Online	Processos	1 Minutos
	Threshold	Crítica Activa		
role_getter-DMS	Measurement	Normal Online	Processos	1 Minutos
	Threshold	Crítica Activa		
synoptics_server-DMS	Measurement	Normal Online	Processos	1 Minutos
	Threshold	Crítica Activa		
sysLogger-DMS	Measurement	Normal Online	Processos	1 Minutos
	Threshold	Crítica Activa		
tag_pin_server-DMS	Measurement	Normal Online	Processos	1 Minutos
	Threshold	Crítica Activa		
tix_sync_server-DMS	Measurement	Normal Online	Processos	1 Minutos
	Threshold	Crítica Activa		
uid_allocator-DMS	Measurement	Normal Online	Processos	1 Minutos
	Threshold	Crítica Activa		
version_manager-DMS	Measurement	Normal Online	Processos	1 Minutos
	Threshold	Crítica Activa		
WSTODESPACHO	Measurement	Normal Online	Processos	1 Minutos
	Threshold	Crítica Activa		
Políticas desactivadas				
event_bridge-DMS	Measurement	Normal Online	Processos	1 Minutos
	Threshold	Crítica Activa		
proxy_bridge-DMS	Measurement	Normal Online	Processos	1 Minutos
	Threshold	Crítica Activa		

As mensagens geradas por estas políticas são monitorizadas directamente pelo operador, através da árvore de nós, sendo as mesmas filtradas por uma regra de cálculo com base no processo 'NetState-DMS de onde se determina o estado actual do equipamento, ou seja se este se encontra em operação ou em reserva.

Os processos da Tabela 4.7 fazem parte de uma listagem de processos considerados como críticos pela empresa EFACEC.

4.4.5. HIM

Os servidores HIM, ou servidores de bases de dados de históricos, são equipamentos que executam uma base de dados Oracle, sobre uma plataforma Microsoft Windows XP. Estes equipamentos centralizam e registam toda a informação gerada pelo normal funcionamento do sistema de controlo, bem como contêm as tabelas de configuração de todos os equipamentos actualmente a serem controlados pela rede. Configurações que são novamente transferidas para os equipamentos a quando de uma sincronização ou controlo geral.

Uma vez que se trata do núcleo de informação é exigido destes equipamentos um elevado nível de fiabilidade, e disponibilidade. Como tal a monitorização por parte da ferramenta HP-OpenView é executada em vários níveis, não observando apenas o sistema operativo e os processos em execução, mas também os processos são mapeados na árvore de serviços.

De registar que a empresa EDP não tem o agente de monitorização de bases de dados Oracle existente e comercializado pela HP, sendo que a avaliação do funcionamento da base de dados será efectuado por análise de processos como mostrado na Tabela 4.8 e na Tabela 4.9.

Tabela 4.8 - Processos HIM Online

Processo	Nº de Processos	Mensagem	Serviço
Políticas estudadas			
oracle	1	Crítica	BD Oracle
cluster_tool	1	Crítica	GENESys
him_wrapper	1	Crítica	GENESys
load_forecast	1	Crítica	GENESys
event_bridge	16	Crítica	GENESys
navigator	1	Crítica	GENESys
node_manager	1	Crítica	GENESys
sysLogger	1	Crítica	GENESys
db_channel	16	Crítica	db_channel
Política desactivada			
nn_engine	1	Crítica	GENESys

Tabela 4.9 - Processos HIM Standby

Processo	Nº de Processos	Mensagem	Serviço
Políticas estudadas			
oracle	1	Crítica	BD Oracle
cluster_tool	1	Crítica	GENESys
him_wrapper	1	Crítica	GENESys
load_forecast	1	Crítica	GENESys
event_bridge	1	Crítica	GENESys
navigator	1	Crítica	GENESys
node_manager	1	Crítica	GENESys
sysLogger	1	Crítica	GENESys
Política desactivada			
nn_engine	1	Crítica	GENESys

4.4.5.1. Processos BD Oracle

Por observações ao comportamento da base de dados pode-se dizer que o processo Oracle é um processo core no funcionamento normal da base de dados, sendo o mesmo necessário para garantir que as bases de dados estejam em funcionamento e para que as *query's* sejam efectuadas com sucesso.

4.4.5.2. Processos db_channel

Os processos db_channel são responsáveis pela disponibilização das tabelas constantes na base de dados desta feita existe um processo e execução por cada tabela que esteja em funcionamento.

4.4.5.3. Processos GENESys

Os processos GENESys garantem a inserção e consulta das bases de dados, da comunicação aos equipamentos da informação de qual a HIM em funcionamento. E efectuam a comutação no estado das HIM de em serviço para reserva e de reserva novamente para serviço. Os processos GENESys também efectuam registos de eventos nos dois equipamentos independentemente de este se encontrar em serviço ou em reserva.

4.4.6. Postos de Operação (BWS e WS)

Os postos de operações são compostos por computadores normais com a aplicação GENESys a ser executada, bem como por *blades* de um servidor HP Itanium com a sua estrutura repartida emulando vários equipamentos em que cada um destes equipamentos executa a aplicação GENESys, a estes centros de processamento é depois associada uma ligação por HP-RemoteGrafics Software, ligação esta que é posteriormente acedida por computadores com um sistema operativo Linux, de onde os funcionários efectuam a monitorização e o controlo dos equipamentos de rede.

Estas máquinas desempenham um dos papéis vitais para no modelo de negócio da EDP, pois são os pontos de acesso e de controlo de toda a rede eléctrica de Portugal, sendo que actualmente existem duas redes para controlo da rede norte e da rede sul. A criação destas redes deve-se a garantir o isolamento funcional da rede sendo que uma avaria no controlo de uma rede não terá influência nos serviços da outra. Esta solução encontra-se em processo de alteração podendo já em vários equipamentos se efectuar a monitorização das duas redes, as vantagens serão a possibilidade de um centro de comando assumir a gestão do subsequente.

De se realçar nos equipamentos que uma intervenção nestes postos não é pois possível via HP-RemoteGrafics sem o conhecimento do seu utilizador e sem que o mesmo pare de executar as suas funções, durante o referido acesso. Por estas razões qualquer anomalia que provoque uma inutilização do equipamento poderá ter custos elevados para a empresa. Sendo que a definição gestão destes equipamentos reflecte uma utilização crítica pois se a meio de uma operação de comando se perder o acesso á plataforma de controlo, poder-se á provocar quebras no serviço ao cliente final.

Tendo em conta a importância de estes equipamentos estarem disponíveis 24 horas por dia 7 dias por semana, os mesmos são monitorizados pelos agentes do HP-OpenView, em busca de possíveis pontos de anomalia que provoquem o quebra de serviço. Como tal nestes postos de operação são tidos em conta vários factores, tais como a performance e fiabilidade. Sendo constantemente efectuada uma manutenção preventiva, os mesmos encontram-se sob vigilância diária, garantindo o seu melhor desempenho possível.

Tabela 4.10 – Processos no Posto de Operações (BWS e WS)

Designação	Tipologia	Mensagens geradas	Variável a ser monitorizada	Intervalo de inspecção
Políticas estudadas				
Operator_notebook	Measurement Threshold	Normal Online Crítica Activa	Processos	1 Minutos
Gis_magik	Measurement Threshold	Normal Online Crítica Activa	Processos	1 Minutos
SW_to_bus	Measurement Threshold	Normal Online Crítica Activa	Processos	1 Minutos
java_ws	Measurement Threshold	Normal Online Crítica Activa	Processos	1 Minutos
Edit_screen_manager	Measurement Threshold	Normal Online Crítica Activa	Processos	1 Minutos
AlarmList	Measurement Threshold	Normal Online Crítica Activa	Processos	1 Minutos
Browser_historical_him	Measurement Threshold	Normal Online Crítica Activa	Processos	1 Minutos
Draw	Measurement Threshold	Normal Online Crítica Activa	Processos	1 Minutos
Events_distributer	Measurement Threshold	Normal Online Crítica Activa	Processos	1 Minutos
Node_Manager	Measurement Threshold	Normal Online Crítica Activa	Processos	1 Minutos
proxy_bridge	Measurement Threshold	Normal Online Crítica Activa	Processos	1 Minutos
WSTOHIM	Measurement Threshold	Normal Online Crítica Activa	Ligação de rede	1 Minutos
LINK_DMS_HIM	Scheduled Task	Normal Online Crítica Activa	Processos	1 Minutos
sysLogger	Measurement Threshold	Normal Online Crítica Activa	Processos	1 Minutos
Sequence_Monitor	Measurement Threshold	Normal Online Crítica Activa	Processos	1 Minutos
uid_allocator	Measurement Threshold	Normal Online Crítica Activa	Processos	1 Minutos

WSTODMS	Measurement Threshold	Normal Online Crítica Activa	Processos	1 Minutos
AlarmGenerationStatus	Measurement Threshold	Normal Online Crítica Activa	Processos	1 Minutos
table_notebook	Measurement Threshold	Normal Online Crítica Activa	Processos	1 Minutos
local_context_manager	Measurement Threshold	Normal Online Crítica Activa	Processos	1 Minutos
Bus_to_sw	Measurement Threshold	Normal Online Crítica Activa	Processos	1 Minutos
tags_pins_browser	Measurement Threshold	Normal Online Crítica Activa	Processos	1 Minutos
Políticas desactivadas				
event_bridge	Measurement Threshold	Normal Online Crítica Activa	Processos	1 Minutos
Navigator	Measurement Threshold	Normal Online Crítica Activa	Processos	1 Minutos
Screen_manager	Measurement Threshold	Desactivada	Processos	1 Minutos
toolbox	Measurement Threshold	Normal Online Crítica Activa	Processos	1 Minutos
Políticas Implementadas				
Get_Log_BWS_interligacao	Measurement Threshold	Normal Online Crítica Activa	Processos	1 Minutos
Get_Log_BWS	Measurement Threshold	Normal Online Crítica Activa	Processos	1 Minutos

4.4.6.1. Processo WSTOHIM

A implementação desta política efectua a monitorização da ligação de rede entre o posto de operações e a HIM actualmente em actividade, a mesma baseia-se em dados adquiridos pela tarefa LINK_DMS_HIM.

4.4.6.2. Processo LINK_DMS_HIM

Esta tarefa executa um *batch* script que efectua um ping as maquinas DMS e HIM retornando ao OPCMON o valor TRUE para cada ligação detectada.

4.4.6.3. Processo WSTODMS

Esta política efectua a monitorização da ligação de rede entre o posto de operações e as DMS. Gerando uma anomalia a quando da não detecção do equipamento, baseando-se em dados obtidos por LINK_DMS_HIM.

4.4.6.4. Processo Get_Log_BWS_interligacao e Get_Log_BWS

Estas duas políticas foram criadas com o objectivo de ler o ficheiro de registo dos portos de operações para a base de dados sendo possível a sua análise sem o acesso directo ao equipamento.

A existência de duas políticas para a realização desta tarefa deve-se a existência de postos de operações que efectuam a monitorização das redes norte e sul tendo o referido ficheiro de registo com uma localização diferente.

Capítulo 5

OVOW Ferramentas implementadas

5.1. Mensagens Internas

Na sua génesis, os agentes do HP OpenView, geram várias mensagens de avisos. Tais como, mensagens de politicas cujo tempo de execução não foram cumpridos, ficheiros de registos que se encontram vazios, tentativas de comunicação de dados falhadas e agendadas para um período posterior, entre outras.

Estas políticas, por muito interessantes do ponto de vista de monitorização, para o operador da consola não têm grande relevância podendo mesmo conter informações contraditórias e sendo as mesmas ainda prejudiciais pois fornecem demasiada informação ao mesmo utilizador.

Desta forma tornou-se importante para a empresa EDP a omissão de algumas das mensagens geradas. Com o estudo detecta-se que na realidade estas mensagens são importantes e trazem informação vital, de que existem políticas internas nos agentes sendo executadas em erro facto conhecido pela empresa e cuja relevância não é considerada como sendo crítica.

5.1.1. Politica “Filtro mensagens internas’ já existente.

Como forma de limpar estas mensagens a empresa EDP já havia avançado com a criação de uma política a qual efectua um filtro de mensagens recebidas, filtrando todas as mensagens geradas internamente pelo agente. Tendo em conta a forma de actuação do HP-OpenView, a criação desta política deveria funcionar, produzindo o fim para o qual foi criada, facto que não se encontrava a acontecer.

Após uma análise cuidada a gigantesca quantidade de mensagens deste tipo recebidas, era evidente a não operacionalidade da mesma política.

5.1.2. Novos procedimentos de activação

Este problema levanta várias questões na sua resolução, sendo a primeira destas, o porquê do não funcionamento do filtro já instalado (Figura 5.1), bem como o facto de realmente queremos que estas mensagens desapareçam, não serão as mesmas importantes?

Na resposta a estas questões encontra-se então que o porque do filtro já previamente criado não se encontrar funcional, tendo sofrido ligeiras alterações para executar as funções pretendidas.

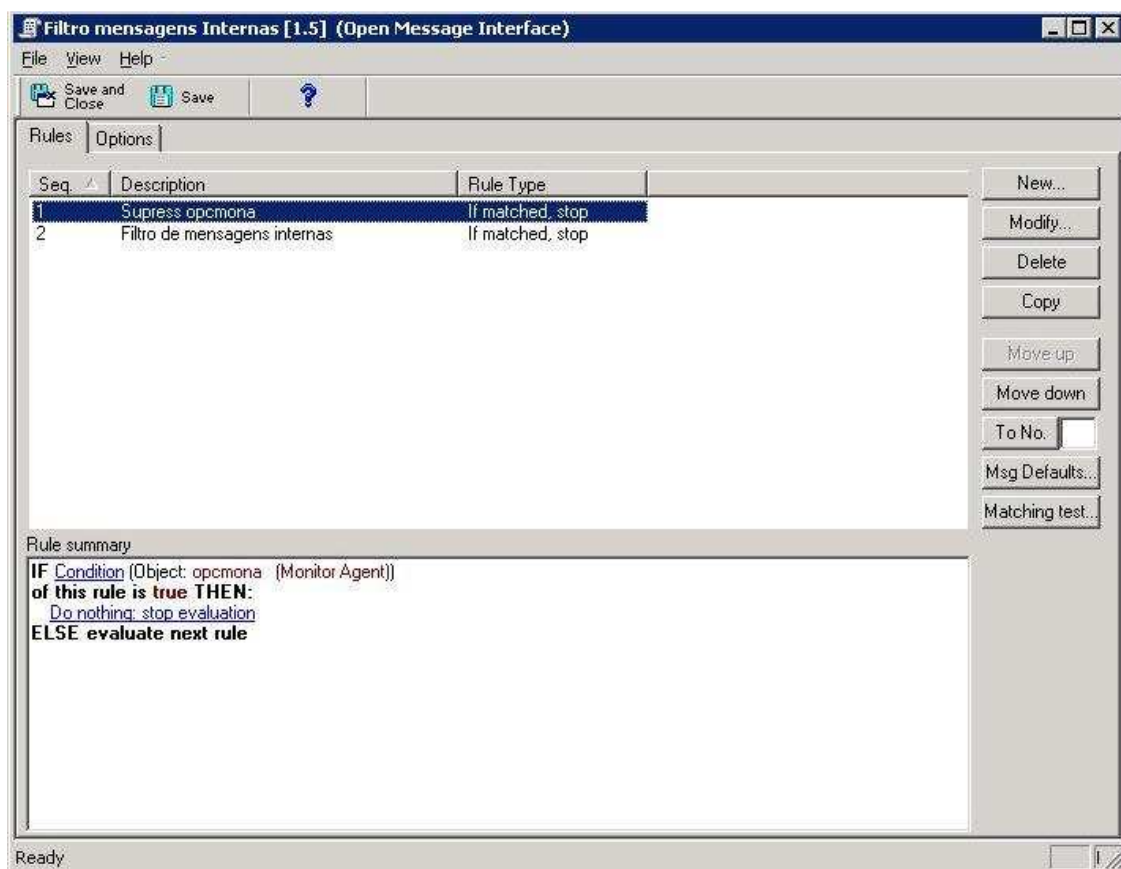



Figura 5.1 - Filtro de mensagens internas

Este filtro, tendo como base a limpeza de mensagens que contenham a palavra "*Internal*", as mesmas são criados pelos agentes e pélo HP-OpenView Operations, e têm informação que poderá ir desde uma política que demorou mais que o esperado a responder até á informação de que o HP-OpenView não consegue contactar o agente.

A condição que leva a que a implementação existente não funcione trata-se de um sistema de segurança inicialmente activado para que este tipo de mensagens seja de

prioridade máxima, ou seja são mostradas directamente ao utilizador sem passarem pelos processos de filtragem tanto dos agentes como do controlo central.

Na resolução do mesmo é necessário então efectuar a alteração do ficheiro de configurações dos agentes “opcinfo” bem como a alteração do ficheiro de configurações, no sistema de controlo central “opcsvinfo”.

```
 1 ################################################################################
 2 # File:          opcinfo
 3 # Description:   Installation Information of ITO Managed Node
 4 # Package:       HP OpenView IT/Operations
 5 # Status:
 6 ################################################################################
 7 OPC_INSTALLED_VERSION A.07.36
 8 SVCDISC_INSTALLED_VERSION A.07.29
 9 PERF_INSTALLED_VERSION A.07.30
10 COMM_INSTALLED_VERSION A.07.19
11 OPC_MGMT_SERVER ccb-ovw.scc-lx.pt
12 OPC_INSTALLATION_TIME 08/06/2008 16:46:19
13 OPC_SG FALSE
14 OPC_NO_CFG_RQST_AT_STARTUP TRUE
15 OPC_EXEC_USER SYSTEM
16 OPC_INT_MSG_FLT TRUE
17
```

Figura 5.2 - Ficheiro de configuração “opcinfo”

Neste ficheiro podemos encontrar dados tais como a versão dos agentes instalados (Figura 5.2 linha 7 a 10), DNS do equipamento em que o HP-OpenView Operations e encontra a ser executado (Figura 5.2 linha 11), a data de instalação dos agentes (Figura 5.2 linha 12). As restantes linhas do ficheiro tratam de variáveis, de onde se destaca a linha 16, esta fora inserida para que o agente reconheça as mensagens internas e efectue a execução dos filtros sobre as mesmas.

Quanto ao ficheiro “opcsvinfo” este não foi alterado pois a sua modificação irá omitir as mensagens de erros na ligação com o agente, mensagens que são de interessante monitorização pois destas se destaca a qualidade de informação a ser visualizada pelo operador.

Uma vez que na EDP existem actualmente mais de 100 equipamentos nestas condições seria um trabalho inglório a alteração manual deste ficheiro e posterior reiniciar do agente correspondente. Nesta lógica de não se ter que aceder a cada máquina para efectuar estas alterações foi criada uma ferramenta em HP-OpenView Operations, que acompanhada de um código em “Shell Script” insere a linha “OPC_INT_MSG_FLT TRUE” nos ficheiros “opcinfo” de cada máquina, executando posteriormente o reinício dos referidos agentes. Nota-se que estes script’s apenas se podem usar em máquinas a executar o sistema operativo Microsoft Windows, nas máquinas que suportam o sistema operativo HP-UX este ficheiros foram alterados manualmente, uma vez que as quatro máquinas existentes não proporcionam a disponibilidade de tempo para a criação de tal script sendo mais vantajoso a sua alteração manual.

5.1.3. Testes de implementação

Antes de se colocar esta política em execução nos mais variados equipamentos efectuou-se uma contagem de mensagens internas produzidas diariamente de onde resultam os seguintes dados.

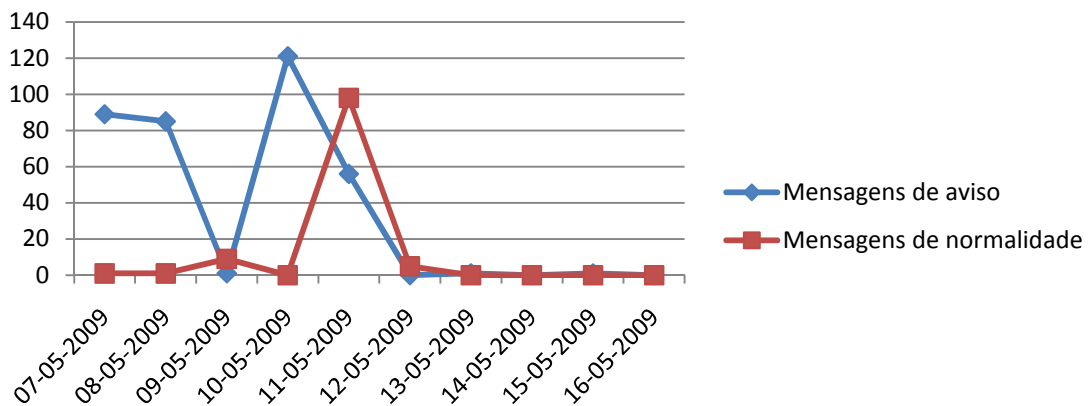



Figura 5.3 - Gráfico da evolução do número de mensagens internas

Do gráfico disposto na Figura 5.3, será de interesse realçar que a implementação da política de limpeza teve lugar no período de 8 a 13 de Maio, sendo que neste período todas as mensagens recebidas foram analisadas e efectuadas alterações ao script inicial.

5.2. Arranque do OVOW

O servidor do HP-OpenView é executado em vários processos de sistema, por omissão existindo vários métodos para se efectuar um reinício dos serviços em caso de anomalia ou mesmo por necessidade. Para tal a HP dispõem de uma ferramenta que permite a realização da paragem e reinício do servidor. Note-se que os serviços podem ser parados efectuando um pedido de sistema com o comando *taskkill* aos processos, situação apenas aconselhada caso o script da HP não funcione.

Como o reinício dos serviços do HP- OpenView Server necessita da inserção de vários códigos na linha de comando foram criados dois executáveis em *batch* script, que auxiliam na paragem e inicio do aplicação servidor e da sua base de dados. Os mesmos scripts encontram-se na raiz "C:\" do equipamento que suporta o servidor da HP.

5.2.1. Paragem do HP-OpenView Servidor

Neste script foram incluídos os comandos:

- vpstat -3 -r stop
- net stop winmgmt

Os quais o primeiro efectua a paragem de todos os serviços do servidor, enquanto o segundo efectua a paragem de todos os protocolos da rede de comunicação com ao Agentes.

5.2.2. Inicio do HP-OpenView

Uma vez o servidor parado existem funções de inicio do mesmo, este início irá lançar novamente todos os processos associados ao funcionamento do HP-OpenView bem como reabrir as ligações de redes para com os agentes. Após este procedimento o servidor inicia uma operação de sincronização com todos os agentes.

- vpstat -3 -r start

A sincronização é efectuada por parte dos agentes enviando as mensagens em memória, iniciando o envio por ordem das mensagens mais antigas para as mais recentes, sendo esta comunicação efectuada apenas durante um período de tempo máximo, passando a comunicação para o agente seguinte, possibilitando assim a comunicação de todos os agentes num tempo considerado aceitável e não prendendo as comunicações apenas a um equipamento quando outras mensagens possam ser prioritárias.

5.3. Apagar políticas nos agentes

Com relativo interesse para futuras actualizações da plataforma encontra-se a limpeza de políticas antigas, estas são recorrentes da situação inicial da rede em que existiam dois equipamentos de monitorização, um no norte e outro no sul. Com a reestruturação da rede e a monitorização apenas por parte de um servidor HP-OpenView, e no decorrer desta operação o servidor do norte foi acrescentado ao existente em Lisboa, não se tendo tido em conta a limpeza inicial das políticas existentes encontrando-se as mesmas ainda em execução nos equipamentos e sendo as mesmas responsáveis pelo aparecimento da grande quantidade de mensagens internas.

Como tal para estabilização da infra-estrutura de mensagens terá que se ter em conta a limpeza dos agentes antes de se confiar nos resultados produzidos pelas mensagens existentes.

Neste contexto é sugerido para resolução do problema a desinstalação do agente e posterior limpeza dos seguintes ficheiros:

Execução do script presente em "%OvAgentDir%\bin\OpC\install\mgmt_sv.vbs”

Apagar a directoria "%OvAgentDir%\conf\ConfigFile\policies" para remover as políticas *ConfigFile* do nó.

Apagar a directoria "%OvAgentDir%\conf\svcdisc\policies" para remover as políticas Service Auto-Discovery existentes no nó.

Apagar a directoria "%OvAgentDir%\conf\nodeinfo\policies" para remover as configurações do ficheiro *Node Info*.

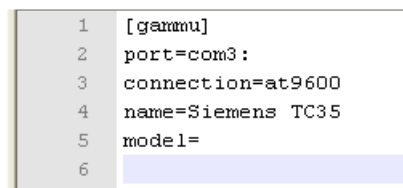
Apagar a directoria "%OvAgentDir%\conf\mgrconf\policies" removendo as políticas *Flexible Management* existentes no nó.

Apagar a directoria "%OvAgentDir%\conf\OpC\vpwin" removendo assim todas as restantes políticas existentes no nó.

Após se ter efectuado este procedimento o mesmo equipamento deverá ser reiniciado e novamente instalado o agente, sendo lhe colocadas todas as políticas que realmente efectuam monitorização.

5.4. Envio de mensagens via GSM

Um dos pontos-chave da plataforma HP-OpenView é a possibilidade de se conectar a vários equipamentos, fazendo uso das propriedades dos mesmos a seu favor e servindo-se das mesmas para que o operador de rede melhor a sua visão em tempo real de todos os acontecimentos relevantes da rede.

Como tal surge a ideia de conexão de um modem GSM ao servidor proporcionando assim em caso de uma anomalia pré-programada o envia de mensagens alertando para um grave acontecimento, o qual exige intervenção imediata por parte dos responsáveis de manutenção.

O modem GSM esteve em anomalia durante os primeiros 2 meses decorrentes do inicio deste trabalho, sendo a avaria detecta a quando de uma deslocação a Lisboa e visualização do equipamento, de onde facilmente se reparou que a avaria era provocada pelo conversor USB/Porta Série que estava visivelmente danificado. O modem foi então retirado do equipamento e transportado para Vila Nova de Gaia local onde este trabalho decorria. Após alteração do cabo danificado o mesmo pode ser então configurado para comunicação com o HP-OpenView.

No actual estado o modem encontra-se ainda em Vila Nova de Gaia sendo que não foi possível o teste da ligação entre o HP-OpenView e o modem. Bem como a implementação de qualquer tipo de política por parte do HP-OpenView no envio de mensagens. No entanto foram efectuados testes ao modem ligando-se o mesmo a outro equipamento, sendo que o mesmo se encontra operacional e parametrizado, enviando mensagens em todos os testes efectuados.

5.4.1. Configuração do modem Siemens TC35

O modem da Siemens TC35, encontra-se parametrizado para uma conexão via porta serie, utilizando o protocolo RS232, possui uma fonte de alimentação (transformador externo), uma antena e uma entrada para um cartão do operador móvel.

A operação com o modem é efectuada em ambiente Windows, usando os seguintes os programas, Wannu para um ambiente gráfico e Gammu num ambiente de desenvolvimento linha de comandos. Sendo que o HP-OpenView irá utilizar a aplicação Gammu. A sua parametrização é realizada por um ficheiro de configuração com o nome 'gammurc' encontrando-se o mesmo presente na directoria '…\gammu\bin\', este ficheiro terá que conter a informação referente a porta onde se encontra ligado o modem, a velocidade de comunicação do computador com o modem, nome do modem e o seu modelo, como se pode visualizar na Figura 5.4.

```
1   [gammu]
2   port=com3:
3   connection=at9600
4   name=Siemens TC35
5   model=
6
```

Figura 5.4 - Ficheiro de configuração do modem GSM

5.5. Gráficos de performance

A activação da consola de gráfico foi proporcionada com a deslocação efectuada, uma vez que a aplicação HP-OpenView não tinha acesso a criação de ficheiros na pasta "\HP-OpenView\Data\Webpages\", sendo este problema causado dor restrições nas permissões, uma vez que a conta de acesso que me fora disponibilizada não tinha permissões para criação de ficheiros na referida directoria.

Após a alteração das permissões do referido directório colocando o mesmo para acesso a todos os utilizadores, foi possível desenvolver um conjunto de gráficos baseados nas variáveis previamente monitorizadas pela política WINOSSPI-WINOS_NT4_Logging e WINOSSPI-WINOS_Win2k_Logging que foram colocadas nos equipamentos no decorrer deste trabalho. Estes gráficos implementados efectuam a amostragem de níveis de utilização do processador, disco e dados de rede como visível na Figura 5.5.

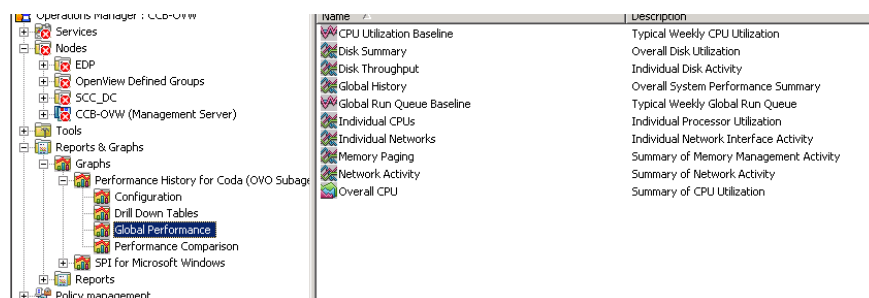



Figura 5.5 – Árvore de gráficos

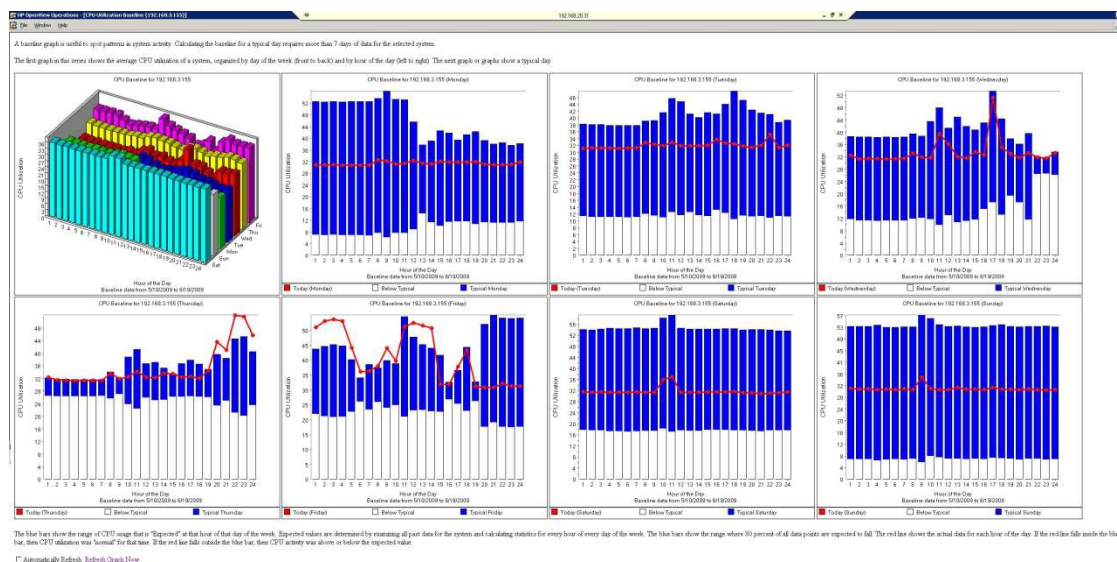



Figura 5.6 – Relatório gráfico modelo criado pela HP

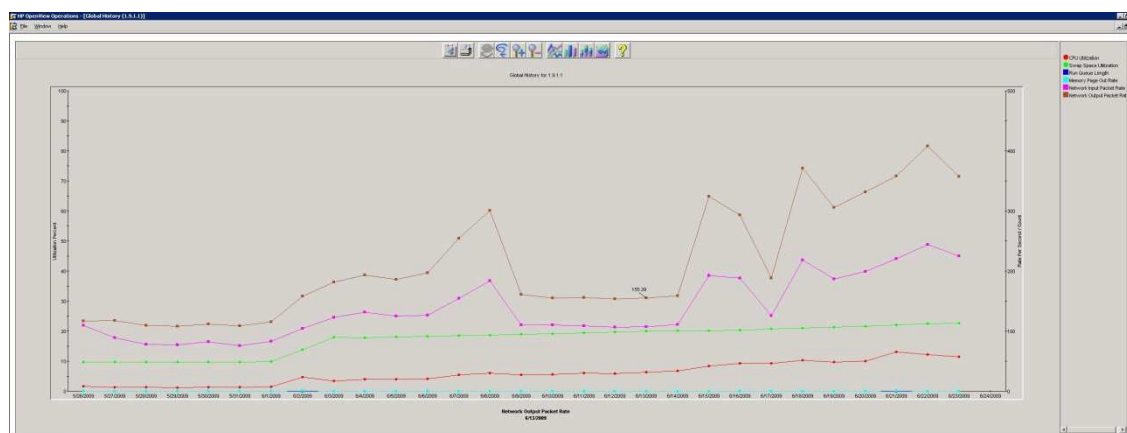



Figura 5.7 – Relatório gráfico de uma DMS criado no decorrer deste trabalho

Estes gráficos Figura 5.6 e Figura 5.7 proporcionam pois uma visão temporal da evolução das performances dos equipamentos, de se notar que o campo temporal foi deixado ao critério do utilizados para que o mesmo possa alterar o período de visualização. Nota-se nos mesmos que apenas é possível efectuar gráficos com início no dia em que a política ficou activa nos equipamentos, ou dos últimos 3 meses, a razão por detrás deste ultimo critério devesse ao facto do acumular de informação, informação esta fica armazenada nos agentes, ou seja nos equipamentos monitorizados.

A informação gráfica obtida por este meio é pois muito útil na implementação de novas actualizações, bem como para a análise do que poderá ter causado um problema. Estes factos levam a uma monitorização das mensagens obtidas, e subsequente análise gráfica da evolução do problema podendo-se retirar várias conclusões sobre a origem da anomalia

5.6. WebInterface

A consola Web (Figura 5.8) disponibilizada o acesso a múltiplos operadores de rede, bem como a subdivisão dos mesmos por várias estruturas e gravidades de mensagens, podendo existir operadores de manutenção cujo interesse recaia apenas sobre o bom funcionamento do hardware e software, e operadores de gestão em que o seu interesse será mais a estrutura e as interligações entre equipamentos.

Nesta consola é apenas possível efectuar a monitorização e execução das mais variadas ferramentas implementadas estando estas associadas a um nó ou a uma mensagem, não sendo pois possível a criação de novas políticas e a colocação destas nos agentes. Não é também possível a execução de ferramentas de apoio que não estejam alocadas a um determinado nó ou mensagem.

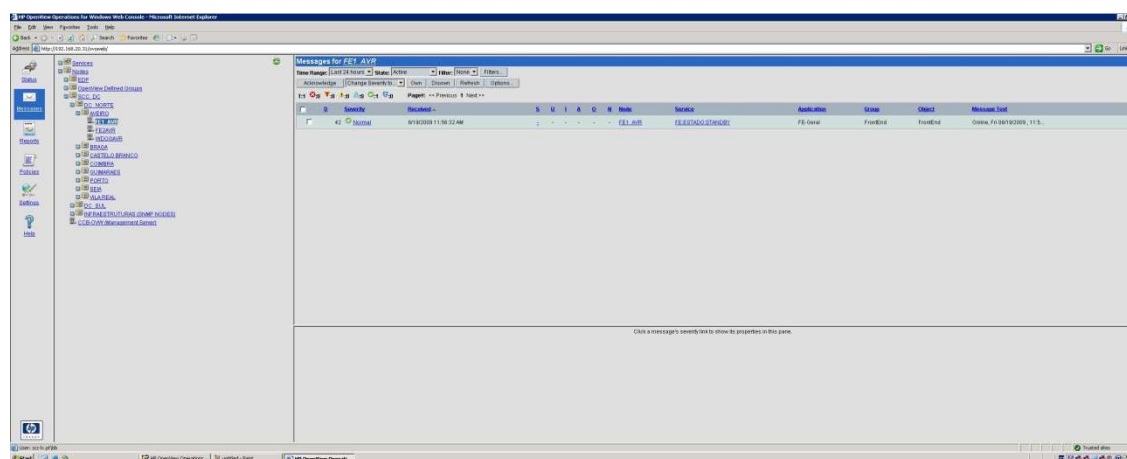



Figura 5.8 – Consola Web do HP-OpenView

5.7. Ligação a base de dados Microsoft SQL Server

A instalação do HP-OpenView nos servidores da EDP contém uma configuração de base de dados externa á normalmente usada pela aplicação. Na instalação padrão é utilizada uma base de dados Microsoft Access, sendo que esta base de dados não é muito versátil pois apenas armazena as mensagens dos últimos sete dias. Como tal o HP-OpenView bem equipado com a possibilidade de se utilizar uma base de dados com características mais avançadas, neste caso foi utilizada uma base de dados Microsoft SQL Server.

Para que se efectue a ligação a esta base de dados existe um mecanismo de transporte de informação, de forma a se duplicar a estrutura interna do HP-OpenView para a base de dados Microsoft SQL Server, bem como posteriores mensagens geradas pela plataforma.

Num primeiro passo existe um script 'OVdbcript.exe' já concebido pela HP com a função de se configurar a base de dados destino. Bem como o utilizador e a palavra-chave de acesso. No HP-OpenView para acesso a base de dados é necessário que a mesma tenha o utilizador padrão 'OVMS_ADMIN'. O HP-OpenView exige um utilizador de base de dados com permissões de administrador, pois este utilizador é utilizado em todos os seus módulos. As configurações da base de dados implementadas são então:

Utilizador:	
Palavra-chave:	

Capítulo 6

Shell Script

Nos sistemas operativos de hoje em dia a quantidade de ferramentas disponibilizadas pelos mesmos torna a tarefa do utilizador algo complexa. Este para além te ter que escolher a melhor ferramenta para a resolução do seu problema ainda tem um grande número de vezes que interligar várias destas ferramentas de forma a obter o resultado pretendido. Esta tarefa torna-se ainda mais monótona se o utilizador tiver que repetir o mesmo processo inúmeras vezes.

No apoio a resolução de problemas e a criação de novas ferramentas, os sistemas operativos surgem com a possibilidade de se executar ficheiros. Estes ficheiros contem nos mesmos, comandos, programas e chamadas de ferramentas, efectuando-se a sua criação como de uma linha de comando se trata-se. Os ficheiros são posteriormente chamados pelo utilizador e o seu conteúdo lançado para a linha de comandos, procedendo assim a sua execução como se fosse o utilizador a inseri-los na linha de comandos.

A utilização deste sistema permite a geração de novas ferramentas, estas tendo como base ferramentas já existentes, possibilitando assim ao utilizador apenas com uma chamada de execução obter o resultado. De notar que estas ordens de execução de ferramentas poderão ser criadas por utilizadores experientes e partilhadas a outros utilizadores, não sendo necessário para os segundos o conhecimento de como se procede a obtenção do resultado, apenas que estas lhes proporcionem esse resultado.

6.1. Microsoft Batch Files

Os ficheiros *batch* permitem a um utilizador do Windows criar listas de comandos, sendo estes comandos executados de forma sequencial, (de cima para baixo), uma vez chamado para execução o referido ficheiro.

Por exemplo um ficheiro *batch* poderá ser usado para efectuar cópias de segurança sempre que se inicia a operação de desligar o computador em ambiente Windows.

Um dos mais conhecidos exemplos deste género de ficheiros é o ficheiro autoexec.bat, que é executado todas as vezes que o Windows inicia. Permitindo a alteração de algumas configurações, e mesmo a própria selecção do sistema operativo que irá ser utilizado.

6.1.1. Criar um Batch file

Os ficheiros *batch* podem ser criados a partir de um editor de texto básico como o Notpad ou o Wordpad. Tendo estes apenas como requisitos que guardados com a extensão ".bat".

Neste editor poderá escrever os comandos, um por linha como se da linha de comandos se trate, sendo que os mesmos serão interpretados de cima para baixo no ficheiro e aguardando o final de execução de um comando para inicio de outro, isto não utilizando comandos como "*start*" e "*run*" que dão início a novos processos independentes.

Uma das mais interessantes utilizações deste género de ficheiros é a possibilidade de se poder ter um conjunto de funções avançadas, sem ser necessário conhecer a forma como estas são tratadas, podendo os mesmos ficheiros *batch* ser executados com o pressionar do rato sobre o mesmo. Proporcionando desta forma a invocação de comandos para execução por parte de utilizadores inexperientes, podendo os mesmos iniciar uma cópia de segurança, execução de um programa com previa limpeza dos dados do utilizador anterior, entre outros.

6.1.2. Implementação de Scripts em Batch file

6.1.2.1. Monitorização de um Processo

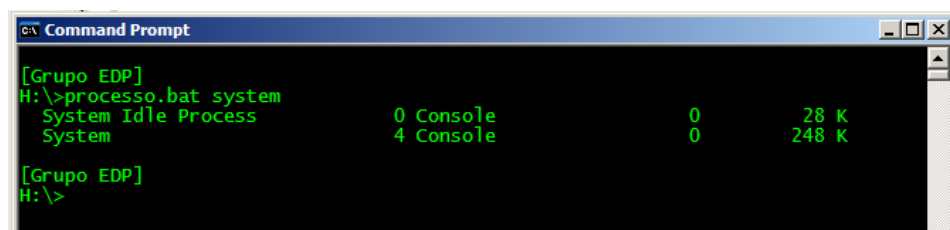
Nesta fase inicial será dada atenção a alguns scripts implementados tendo como finalidade a monitorização de variáveis e/ou processos decorrentes do sistema operativo Microsoft Windows. Uma vez que no decorrer deste projecto estes constituem um elemento fulcral na comunicação com o sistema HP-OpenView Operations.

```
1 @echo off
2 tasklist > lista
3 findstr /n /i %1 lista
4 del lista
5
```

Figura 6.1 – Código que reporta o nome do processo por referência, caso este esteja em execução

Neste exemplo da Figura 6.1 observa-se um código que permite a visualização de um determinado processo, este é útil se o mesmo for chamando pelo HP-OpenView. O HP-OpenView executa o script e analisa a sua resposta neste caso se o mesmo não retornar nada este emite um aviso de processo inexistente. A sua chamada a partir de linha de comandos (Figura 6.2) terá que incluir o nome do processo a verificar, retornando o script uma linha por cada processo com essas especificações encontrado.

```
Command Prompt
[Grupo EDP]
H:\>processo.bat system
  System Idle Process              0 Console             0         28 K
  System                           4 Console             0        248 K

[Grupo EDP]
H:\>
```

Figura 6.2 – Resposta da procura de um processo

O código começa com “@echo off” na linha 1, este comando desactiva o aparecimento de mensagens inúteis, nomeadamente os próprios comandos ao serem lançados para execução. Aparecendo apenas as respostas dos mesmos.

Um elemento que interessa realçar trata-se da possibilidade de comutar a saída de um comando para um ficheiro como se observa na linha 2 com o comando “>”, o qual cria se não existir e insere a resposta do comando “tasklist” no ficheiro com o nome de lista. Esta possibilidade permite-nos em muitas operações manter históricos guardando, respostas sucessivas de um comando.

Outra função também muito útil neste exemplo é o comando “findstr” que associado a um texto procura uma, ou varias correspondentes, podendo no final ter várias respostas conforme dependendo da configuração que o utilizador pretender, neste caso “/n” a linha onde encontre correspondência.

Por fim este apaga o ficheiro, temporariamente criado para armazenar a resposta do comando “tasklist”.

Existe ainda a possibilidade de se poder contar o número de execuções do mesmo processo por parte do HP-OpenView, este para uma comparação de limites de onde o operador de HP-OpenView poderá definir o número máximo de execuções de um processo até este gerar um alarme e o número mínimo de execuções para este ser considerado como critico.

6.1.2.2. Monitorização do estado de um FrontEnd

Uma das mais interessantes monitorizações em termos de serviços por parte do HP-OpenView Operations é o estado actual de um FrontEnd. Permitindo desta forma a visualização de qual destes se encontra em funcionamento e efectuando o registo das comutações entre os mesmos.

Tem ainda a vantagem de se poder determinar a melhor altura para efectuar um reinício do WatchDog, que efectua a monitorização destes FrontEnd's, uma vez que os WatchDog's após um reinício comutam para o FrontEnd principal o que causa uma perda de comunicação com a subestações durante aproximadamente nove minutos até o outro FrontEnd entrar em funcionamento. Se o FrontEnd principal já se encontrar em funcionamento este caso já não acontece, pois a comutação não alterará as ligações, mantendo-se assim as performances de monitorização.

Para avaliação do estado actual dos FrontEnd's estes dispõem de uma consola de controlo e monitorização de várias variáveis.

Utilizando assim este meio de comunicação de informação elaborou-se um script que utiliza a consola retirando e filtrando dados da mesma, possibilitando assim ao HP-OpenView a monitorização do estado em que se encontra o FrontEnd.

6.1.3. Comandos disponíveis

Como os comandos divergem de acordo com as varias versões da *batch* do Microsoft Windows, estes necessitam de ser consultados de acordo com o sistema em que se esta a implementar o script. Uma vez que na EDP apenas se usa sistemas operativos Microsoft Windows XP, Microsoft Windows NT4, Microsoft Windows 2000 Server, e Microsoft Windows 2003 Server.

6.2. Unix Shell Script

O sistema Unix implementado em que se efectuou os testes e criação dos scripts, bem como a sua execução futura, tinha um interface para com o utilizador usando uma kornshell. Esta permite a interface directa entre o utilizador e o núcleo do sistema de uma forma clara e directa, proporcionando desta forma que a interacção decora de uma forma mais intuitiva. Esta consola não implementa interface gráfica sendo apenas um intérprete textual do kernell.

6.2.1. Limpeza de ficheiros de registo do HP-OpenView nas maquina SCADA

Este ficheiro trata-se de um registo residual do script de monitorização de processos já implementado. O script para além de visualizar os processos em execução, adiciona de um em um minuto a verificação efectuado aos processos core. Como a quando da análise não existia nenhum protocolo de limpeza deste ficheiro, desconhecendo-se mesmo a existência e o funcionamento do mesmo, os mesmos tinham tamanhos que variavam de entre ao 170 Megabytes e os 190 Megabytes, ocupando um elevado espaço de disco e tornando o sistema lento todas as vezes que tinha que acrescentar novos dados ao referido ficheiro.

Em análise da situação concluiu-se que seria interessante apenas ter os registos dos últimos sete dias, para análise em caso de avaria. Apagando-se os mesmos no oitavo dia. Esta Solução proporciona a existência de registos de uma forma controlada mantendo o sistema num estado de não crescimento, tem a desvantagem de não ter a informação completa de histórico para períodos anteriores ao sétimo dia, estando apenas a informação de alarmes armazenada na base de dados do HP-OpenView Operations.

Para a realização desta tarefa no HP-OpenView, optou-se pela criação de um evento programado de execução diária as 9:00 horas de cada dia, com a finalidade de apagar o sétimo dia de registos existente na máquina.

Esta tarefa ficou assim associada a um Shell Script que copia de uma forma cíclica o ficheiro de registos do dia anterior para o dia seguinte apagando o do sétimo dia.

Com o decorrer do tempo e na observação da evolução do código deparasse com um compromisso que aquando das chamadas de execução, o mesmo gera ocupação de disco e de processador o gera atrasos no processamento de informação vital tornando este código ineficiente. Tomando em atenção os limites de performance requeridos pelo sistema reavalia-se o código surgindo uma segunda versão do mesmo mais eficiente (Figura 6.3).

```
1  #!/sbin/ksh
2
3  cd /var/opt/OV/tmp/OpC/SCADA
4
5  rm 7SCADA_OPC.log
6
7  mv -f 6SCADA_OPC.log 7SCADA_OPC.log
8  mv -f 5SCADA_OPC.log 6SCADA_OPC.log
9  mv -f 4SCADA_OPC.log 5SCADA_OPC.log
10 mv -f 3SCADA_OPC.log 4SCADA_OPC.log
11 mv -f 2SCADA_OPC.log 3SCADA_OPC.log
12 mv -f 1SCADA_OPC.log 2SCADA_OPC.log
13 mv -f SCADA_OPC.log 1SCADA_OPC.log
14 exit 0
15
```

Figura 6.3 - Limpeza de ficheiros de registos

Esta solução faz uso não de cópias de ficheiros mas sim de alterar características do apontador do ficheiro, o seu nome, apenas apagando o último ficheiro de dados.

Passando assim a existir não um ficheiro de registos mas sim oito de onde a soma dos seus tamanhos se situa entre os 8 Megabytes e os 9 Megabytes

Capítulo 7

Conclusão

7.1. Conclusão

Tratando-se o HP-OpenView de uma ferramenta de desenvolvimento contínuo, a mesma exige uma intervenção diária deixando desta forma a possibilidade de se retirar conclusões mais avançadas apenas para o operador diário.

A avaliação do trabalho desenvolvido no tempo em que decorreu este trabalho é então analisada de uma forma pontual sendo que as futuras operações e desenvolvimentos da rede interna da EDP iram determinar a utilidade das políticas e ferramentas desenvolvidas.

Do objectivo inicial de limpeza das mensagens internas, e com o decorrer do tempo desde a sua implementação em vários equipamentos para teste até a edição deste texto, não se detectou que as mesmas mensagens fossem mostradas ao operador, bem como que a sua omissão tenha de alguma forma contribuído para a falha na detecção de anomalias, ou pontos de estrangulamento, não sendo este um motivo para se deixar de continuar a avaliar esta situação, sendo mesmo recomendado a reinstalação e limpeza dos agentes em equipamentos mais críticos e que emitam um elevado número deste género de mensagens.

Um outro objectivo ao qual estava sujeita a realização no decurso deste trabalho, foi a identificação e monitorização da nova actualização na plataforma GENESys, sendo implementadas várias políticas para monitorização dos novos processos, inactivação de processos descontinuados e actualização de valores em algumas políticas de comparação numérica. Com esta implementação a estrutura GENESys ficou estabilizada na árvore de estrutura dos nós sendo que apenas se efectuou a actualização da estrutura na árvore de serviços para todos equipamentos exceptuando os FrontEnd's e os WatchDog's, isto devido a sua independência uns dos outros não sendo possível a criação de uma política genérica que englobe os processos dos equipamentos identificando o estado actual do mesmo.

Fora ainda um dos objectivos a criação de ferramentas que proporcionassem uma mais fácil manutenção, bem como a activação e estudo das plataformas de emissão de gráficos de performances, e da consola Web. De onde se veio a notar após activação e implementação de várias ferramentas a sua especificidade para com um grupo de equipamentos, sendo realizada uma tarefa de indexação de ferramentas a nós onde as mesmas poderiam ser executadas, possibilitando desta forma um acesso mais rápido a execução da ferramenta bem como a prevenção de execução da mesma em equipamento não apropriado. A construção de gráficos, após a activação da consola veio-se a revelar com um elevado interesse para avaliação do equipamento quando detectada uma anomalia bem como de uma ferramenta de elevado poder no desenvolvimento e determinação de erros de programação.

Na globalidade é facilmente visível a melhoria produzida pela implementação, sendo que actualmente a plataforma se situa num estado de desenvolvimento e amadurecimento para adaptação e ajuste as necessidades requeridas pela rede de comunicações e de equipamentos da EDP. Nota-se a relutância no desenvolvimento gradual do HP-OpenView, uma vez que a plataforma tem sido alvo dos mais variados projectos de estágio, não tendo como tal uma evolução continuada.

7.2. Implementação futura

Futuramente e com a proposta da EDP em aumentar o número de equipamentos monitorizados, actualmente a EDP detêm uma licença para 95 agentes, podendo-se assim efectuar a monitorização de todas as BWS e WS existentes na rede, isto proporcionando um incremento nas performances dos requisitos projectados para a plataforma.

É ainda chamada a atenção para uma futura actualização do hardware do Servidor da plataforma HP-OpenView, isto tendo em conta que a capacidade de disco lógico se encontra num nível crítico.

Outra das possíveis implementações futuras, será a reestruturação da árvore de serviço passando esta a reflectir o estado actual de cada FrontEnd, bem como as anomalias produzidas pelos WatchDog's tendo-se desta forma uma informação para a possibilidade de se poderem afectar comutações entre os FrontEnd's em caso de avaria.

Anexos

Alguns comandos disponíveis em ambiente Microsoft Windows batch.

ADDUSERS	Adiciona uma lista de utilizadores de ou para um ficheiro CSV
ARP	Mostra e altera o IP físico da máquina
ASSOC	Mostra extensões conhecidas e altera extinções de ficheiros
AT	Cria um calendário de tarefas a executar
ATTRIB	Altera atributos do ficheiro
BOOTCFG	Altera parâmetros de arranque do Windows
CACLS	Altera permissões do ficheiros
CALL	Executa um ficheiro Batch
CD	Muda directório
CHKDSK	Ferramenta que verifica anomalias nos discos
CHKNTFS	Mostra o tipo de formatação ou altera a formatação do disco
CIPHER	Encriptação de ficheiros
CleanMgr	Ferramenta que limpa automaticamente ficheiros temporários
CLS	Limpa o ecrã da shell
CMD	Inicia uma nova shell
COLOR	Altera as cores da shell
COMP	Compara dois ficheiros
COMPACT	Mostra ou altera a compressão de um ficheiro NTFS
CONVERT	Converte ficheiros de NTFS em FAT e o inverso
COPY	Copia um ou mais ficheiros
DATE	Mostra e altera a data actual
DEFRAG	Desfragmentação do disco
DEL	Apaga ficheiro
DISKCOMP	Compara o conteúdo de dois discos
DISKCOPY	Copia o conteúdo de um disco

DISKPART	Particiona o disco
DOSKEY	Edita linhas de comando, chama comandos antigos e cria macros
ECHO	Imprime na shell
ENDLOCAL	Apaga as variáveis temporárias criadas na sessão
ERASE	Apaga um ou mais ficheiros
EXIT	Fecha a shell actual
EXPAND	Descomprime ficheiro
FC	Compara dois ficheiros ou directorias
FIND	Procura um texto num ficheiro
FINDSTR	Procura várias ocorrências de um texto num ficheiro
FOR	Comando de execução cíclica
FORMAT	Formata o conteúdo de um disco ou partição
FSUTIL	Feramenta de gestão de discos, atribuição de cota
FTP	Conecta-se usando o protocolo FTP a um Host
FTYPE	Mostra ou altera o tipo de ficheiro
GOTO	Comando de salto na execução de um ficheiro Bach
HELP	Ajuda, lista de comandos possíveis
IF	Função de comparação e decisão
IPCONFIG	Configuração de parâmetros da ligação de rede
LABEL	Atribuição de um atalho ou de um nome
LOGOFF	Termina a secção do utilizador
MEM	Mostra a utilização da memória
MD	Cria um directório
MODE	Configuração de dispositivos de sistema como porta serie
MORE	Mostra o resultado de uma operação um ecrã de cada vez
MOUNTVOL	Configura o volume de um novo disco
MOVE	Move um ficheiro ou directoria
MSG	Envia uma mensagem a um utilizador
MSIEXEC	Aplicação de instalação da Microsoft
MSTSC	Ferramenta de RemoteDesktop
NET	Gestor de recursos de rede
NETSH	Configurador de protocolos de rede
NBTSTAT	Estatísticas de rede NetBIOS over TCP/IP
NETSTAT	Estatísticas de rede TCP/IP
NSLOOKUP	Mostra IP do servidor de rede
NTBACKUP	Ferramenta que efectua copias de segurança
PATH	Caminho de procura

PATHPING	Localiza caminho seguido e pacotes perdidos
PAUSE	Suspende a execução de um script
PERFMON	Mostra o monitor de instrumentação e performance WMI
PING	Testa uma determinada ligação de rede
POPD	Volta a directoria salva em PUSHD
PRINT	Imprime um ficheiro de texto
PRNCNFG	Mostra ou altera a configuração da impressora
PRNMNGR	Lista , adiciona e apaga impressoras
PROMPT	Altera a linha de comando
PsExec	Executa um processo remotamente
PsFile	Mostra ficheiro remoto
PsGetSid	Mostra a SID de um computador remoto ou de um utilizador
PsInfo	Lista de informações do sistema
PsKill	Termina um processo num computador remoto
PsList	Mostra a lista de processos de um computador remoto
PsLoggedOn	Identifica que se encontra a utilizar determinado sistema
PsLogList	Registo de utilizadores
PsPasswd	Alteração de palavra pass de um dado utilizador
PsService	Lista e controla serviços num equipamento remoto
PsShutdown	Desliga ou reinicia um equipamento remotamente
PsSuspend	Suspende processo remoto
PUSHD	Salva o directório corrente
RASDIAL	Configura modem de marcação por impulsos
RASPHONE	Configura modem de marcação por impulsos
RECOVER	Recuperação de ficheiro danificado
REG	Lê, cria e altera chaves do registo de sistema
REGEDIT	Lê, cria e altera as configurações das chaves de registo
REGSVR32	Activa ou inactiva uma biblioteca “DLL”
REGINI	Altera as permissões de acesso aos registos
REM	Grava uma serie de comandos e guarda num ficheiro batch
REN	Altera o nome de um ficheiro
REPLACE	Substitui um ficheiro por outro
RD	Apaga directório
ROUTE	Altera tabelas de routeamento
RUNAS	Executa programa usando uma conta diferente
SC	Controlo de serviços por linha d comando
SCHTASKS	Cria uma tarefa repetitiva usando a linha de comandos

SET	Lista e altera variáveis de sessão
SETLOCAL	Lista e altera variáveis da sessão actual
SHIFT	Muda a posição dos parâmetros de entrada de funções
SHUTDOWN	Desliga, reinicia e termina sessão
SORT	Reordena entradas
START	Inicia programa ou comando numa nova sessão
SUBST	Associa um atalho com uma unidade lógica
SYSTEMINFO	Lista informação do sistema
TASKLIST	Lista processos activos
TASKKILL	Termina processo
TIME	Lista, altera a hora do sistema
TITLE	Altera o título da janela de sessão
TREE	Visualização gráfica de directórios
TYPE	Imprime na shell o conteúdo de um ficheiro
VER	Lista a versão do sistema
VERIFY	Verifica se um ficheiro foi devidamente salvo
VOL	Lista informação do disco lógico
WINMSD	Diagnostico do sistema operativo
WMIC	Comandos da consola WMI
XCOPY	Copia ficheiros e directórios

Alguns comandos disponíveis em ambiente UNIX

AC	Lista o tempo de sessão de um utilizador
AT	Agenda de tarefas a serem realizadas periódica ou esporadicamente
basename	Mostra o comando inicial de uma string
batch	Executa um ficheiro de script em paralelo com a sessão
captoinfo	Conversão de ficheiros
cmp	Compara dois ficheiros
cut	Remove texto seleccionado de ficheiro ou variável de sessão
date	Lista ou altera a data e hora do sistema
iag	Procura problemas de hardware
diff	Compara ficheiros de texto
errclear	Apaga mensagens no registo de erros
errpt	Gera mensagens no registo de erros
fastboot	Reinício rápido

fasthalt	Pausa o sistema
find	Procura correspondência em nomes de ficheiro
grep	Procura correspondência em ficheiros de texto
head	Lista as primeiras 10 linhas de um ficheiro de texto
id	Lista a identidade do utilizador
last	Lista informação das últimas sessões
login	Inicia uma nova sessão
logout	Termina sessão actual
lsitab	Insere processos do arranque do sistema
lslicense	Lista do número de utilizadores que podem se encontrar ligados
kill	Envia um sinal a um processo para parar
nl	Inserem o número de linha num ficheiro
nice	Atribui prioridade a um processo
nvdmetoa	Converte ficheiros EBCDIC em ASCII
od	Altera o conteúdo de um ficheiro para ASCII, HEX, OCT
mitab	Remove processos do arranque do sistema
sed	Comando para alterar texto
shutdown	Desliga equipamento
split	Parte um ficheiro em partes mais pequenas
stopsrc	Para todos os processos do SRC - *System Resource Controller*.
strip	Remove tabela de símbolos
su	Autentificação como *superuser*
sum	Efectua o somatório de um ficheiro
tail	Lista as ultimas 10linhas de um ficheiro
tee	Captura o resultado de um processo

Referências

[1] Abreu, Jaime; Simões, Pedro - "Manual de Procedimentos Network Node Manager". Versão 2.0 de 22 de Agosto de 2005.

[2] Allen, William, Allen, Linda – "Batch File Course". Disponível em http://www.allenware.com/icsw/icswidx.htm. Acesso em 17/Abril/2009.

[3] EFACEC Automação – "GENESys Manual do Administrador: Processos do Sistema", V1.4, ASDV06000301

[4] Helder Ferreira ATDC – "DOCUMENTAÇÃO DE SUPORTE À IMPLEMENTAÇÃO DO HP OPENVIEW NOS EQUIPAMENTOS DE SISTEMAS DE COMANDO ECONTROLO", V1.13

[5] USA BMC, "BMC performance management - datasheet"

[6] USA Hewlett- Packard Development Company, L. P. – "HP OpenView Integration Pack", Part Number: 162-00285-01

[7] "Information on batch files". Disponível em http://www.computerhope.com/batch.htm. Acesso em 17/Abril/2009.

[8] USA Hewlett- Packard Company – "HP OpenView for Windows Fundamentals Student Workbook". Versão B.00 H6778S. USA 04/02.

[9] USA Hewlett- Packard Development Company, L. P. - "HP OpenView network node manager managing your network". Versão T2490-90024 de Julho de 2004

[10] USA Hewlett- Packard Development Company, L. P. - "HP OpenView network node manager scalability and distribution". Versão T2490-90025 de Julho de 2004

[11] Nortel Networks – "Solution Brief Nortel Unified Communications Management", NN124084-042409

[12] USA IBM Corporation – "IBM Tivoli Monitoring", TID14003-USEN-00